RESUMEN – TRABAJO DE GRADO

AUTORES	JEAN CARLOS GARCÍA GUARÍN y DINA LUZ OROZCO CANTILLO
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
DIRECTOR	Mag. GENNY TORCOROMA NAVARRO CLARO
TÍTULO DE LA TESIS	DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

RESUMEN
(70 palabras aproximadamente)

EL TRABAJO PROPONE UNA GUÍA PARA EL USO Y LA APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013. SE ACUDIÓ A LA INVESTIGACIÓN CUALITATIVA COMPRENDER LAS CARACTERÍSTICAS DE LOS ELEMENTOS QUE PARTICIPAN EN EL DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013.

CARACTERÍSTICAS

PÁGINAS: 120	PLANOS:	ILUSTRACIONES: 4	CD-ROM: 1

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

AUTORES:

JEAN CARLOS GARCÍA GUARÍN

DINA LUZ OROZCO CANTILLO

Trabajo de Grado para Optar el Título de Especialista en Auditoría de Sistemas

Directora

GENNY TORCOROMA NAVARRO CLARO

MAG. DIRECCIÓN ESTRATÉGICA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia **Agosto, 2016**

DEDICATORIA

Dedico esta tesis a DIOS, al espíritu Santo, quienes inspiraron mi espíritu para la conclusión de esta especialización.

A mi madre Margarita. Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor. A mi padre Carlos. Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor. Ellos quienes me dieron vida, educación, apoyo y consejos para concluirla.

Mis abuelas Gilma Trujillo (QEPD) E Isabel Rodríguez, por quererme y apoyarme siempre, esto también se lo debo a ustedes.

A mi hermana Sandra por ser el ejemplo de una hermana mayor por ser mi niña especial y del cual aprendo todos los días; a mi hermana María de los Ángeles por llegar en el momento indicado para llenar de alegría nuestros días, a mi hermano del alma, Leonardo, sé que desde el cielo me guías en cada momento de mi vida. A través de tu ausencia física, Dios me ha enseñado que la muerte pertenece a la vida terrenal, como la vida terrenal pertenece a la muerte, y así es que en medio del dolor de no tenerte, igual estas siempre, como mi hermano invisible.

A mi hijo, Anthony, por siempre ser mi compañía, por quererme y demostrármelo en cada mensaje y apoyarme en mis estudios sabiendo que esta gran distancia que nos separa es por un buen futuro, espero ser tu ejemplo para mis nietos.

A mis compañeros de estudio, a mis maestros y amigos especial a ti Leydi, a la profesora Magreth Rossio Sanguino Reyes quien sin su ayuda y asesoría nunca hubiera podido hacer esta tesis. A todos ellos se los agradezco desde el fondo de mi alma.

Jean Carlos García Guarín

DEDICATORIA

Esta tesis se la dedico a Dios por ser mi guía en este proyecto, a mi Familia que ha sido mi motor y mi más grande apoyo en todos los momentos de mi vida, a ti cielo por estar incondicionalmente a mi lado y a mis amigos por compartir mis triunfos, a todos infinitas gracias por estar a mi lado y ser parte de todo esto.

Dina Luz

AGRADECIMIENTO

En primer lugar, queremos agradecer a la Magíster Genny Torcoroma Navarro Claro, por el aporte invaluable y el apoyo constante que nos brindó como Directora del trabajo.

En segundo lugar, queremos agradecer a la Universidad Francisco de Paula Santander Seccional Ocaña por brindarnos la oportunidad de estudiar y formarnos como Especialistas en Auditoría de Sistemas.

Finalmente, queremos agradecer a Magreth Rossio Sanguino Reyes, por el acompañamiento y aportes hechos en este proceso de formación

Índice

Lista de Figuras

Pág.

Lista de Cuadros

Pág.

Lista de Apéndices

Introducción

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades ((ICONTEC), 2006).

La información puede existir de muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando cualquier otro medio; independientemente de la forma que tome la información, o el medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

Para poder materializar esta protección, se hace necesario implementar mecanismos para garantizar que la información utilizada o generada como producto de las actividades organizacionales, está debidamente asegurada y que las amenazas a las que se encuentra expuesta, son valoradas y tratadas eficientemente.

La seguridad de la información se logra implementando un adecuado conjunto de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de

seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

El presente trabajo permitió, realizar un diagnóstico del estado actual de KARISALUD IPS LTDA, en lo relacionado con la seguridad informática y de información, de tal modo que se pudiera realizar una serie de recomendaciones a través de una guía de criterios de aplicabilidad en gestión de la seguridad de la información, de acuerdo con el estándar ISO/IEC 27002:2013.

En lo que tiene que ver con el presente documento, éste se estructuró de la siguiente manera: en un primer capítulo, se plantea el problema identificado, los objetivos, la justificación y las delimitaciones de la propuesta planteada.

En el segundo capítulo, se muestra el Marco Referencial. En él se sustenta la necesidad de implementar controles para la seguridad de la información, de tal forma que KARISALUD IPS LTDA., pueda administrar eficientemente sus recursos informáticos y de información. En el tercer capítulo, se socializa el diseño metodológico propuesto para la realización de la investigación.

En el cuarto capítulo, se presentan los resultados; en primera instancia, se muestra el diagnóstico de la Institución en mención, en lo concerniente a la existencia y eficiencia de controles de seguridad de la información, para lo cual fue necesario, realizar una auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013; seguidamente, se realizó un análisis de

riesgos, identificando las amenazas y vulnerabilidades de la empresa y determinando el nivel de riesgo potencial para la misma; finalmente, se diseñó la guía de aplicabilidad de seguridad de la información de acuerdo como lo contempla el estándar anteriormente mencionado.

Finalmente, el quinto y sexto capítulos, recogen las conclusiones y recomendaciones derivadas de la investigación.

Capítulo 1. Diseño de una Guía De Aplicabilidad de Controles de Seguridad para la Ips Karisalud Ltda De Acuerdo con el Estándar Iso/Iec 27002:2013

1.1. Planteamiento Del Problema

KARISALUD IPS LTDA es una institución prestadora de servicios en salud, orientada a contribuir con el mejoramiento de la calidad de vida de sus usuarios. Tiene como actividad principal la práctica médica sin internación, actividad secundaria, apoyo diagnóstico y actividad adicional, comercio al por menor de productos farmacéuticos y medicinales, cosméticos y artículos de tocador en establecimientos especializados.

Atiende usuarios de régimen subsidiado y contributivo. Sus funciones se basan en asesorar, administrar, elaborar, ejecutar y vigilar los servicios habilitados en el área de la salud. Incluyendo acciones de detección temprana y protección específica, acciones asistenciales y preventivas de baja y mediana complejidad enfocadas a grupos especiales, susceptibles de morbimortalidad.

Los servicios ofertados de baja y mediana complejidad por KARISALUD IPS LTDA son: medicina general, odontología general, promoción y prevención, toma de muestra y laboratorio clínico, nutrición, psicología, terapia respiratoria, fisioterapia, terapia ocupacional, fonoaudiología y especializado en los siguientes campos: medicina interna, gineco-obstetricia, pediatría, cirugía general y ortopedia y/o traumatología.

Dada la cantidad de actividades que desarrolla la IPS en virtud de su objeto social, se genera mucha información que requiere distintos niveles de confiabilidad y confidencialidad, tanto para la empresa como para los usuarios, por lo que se hace necesario avanzar en procesos tendientes a salvaguardar la misma. Sin embargo, muchos de los usuarios se quejan de pérdida de datos relacionados con su historia clínica, alteración de información, duplicidad de la misma, lo cual ha derivado en algunos diagnósticos equivocados, ocasionando situaciones en las que se asigna la misma cita a un usuario en diversas horas del día o en distintos períodos de tiempo.

Por esta razón, la gerencia de la IPS viene adelantando acciones con el fin de diagnosticar el estado actual de su sistema de información y de los controles de seguridad implementados, con el ánimo de garantizar un adecuado manejo de la información que se utiliza en los distintos procesos de la entidad.

Actualmente la IPS KARISALUD Ltda., no cuenta con un modelo de gestión de la seguridad de su información que le permita implementar medidas tendientes a proteger sus recursos informáticos y de información y a aplicar adecuadamente controles de seguridad que permitan ofrecer mejores servicios en cuanto al uso de los datos de sus usuarios y de la entidad como tal.

1.2. Formulación del Problema

¿Qué estrategia se puede implementar para garantizar una adecuada implementación de controles de seguridad en la IPS KARISALUD Ltda.?

1.3. Objetivos

1.3.1. General. Diseñar una guía de aplicabilidad de controles de seguridad para la IPS KARISALUD Ltda., de acuerdo con el estándar ISO/IEC 27002:2013.

1.3.2. Específicos. Realizar un diagnóstico del estado actual de la IPS KARISALUD Ltda., en términos de seguridad informática y de la información, mediante el estándar ISO/IEC 27002:2013.

Realizar un análisis de riesgos de los activos de información de la IPS KARISALUD Ltda.

Elaborar un documento de buenas prácticas de gestión de seguridad de la información de acuerdo con lo establecido en el estándar ISO/IEC 27002:2013.

1.4. Justificación

La mayoría de las instituciones prestadoras de salud, independientemente de la cantidad de usuarios que atienden, almacenan, procesan o distribuyen información a través de su sistema de información, generalmente en forma digital, lo cual, abre la posibilidad a distintas amenazas de

índole virtual o física, por lo que para dichas entidades se hace necesario garantizar su protección, así como la de todo el soporte tecnológico de la misma. Esta medida debe cumplir con los estándares internacionales que para el efecto se han diseñado, siendo el estándar ISO 27001:2013 el más reconocido y aceptado, a fin de garantizar la confidencialidad, la integridad y la disponibilidad de la información procesada.

La IPS KARISALUD Ltda., ha venido de manera permanente fortaleciendo diversas estrategias a fin de garantizar la calidad tanto de los servicios que presta como aquellos que se relacionan con su gestión institucional. Por esta razón, desde la gerencia de la IPS se adelantan acciones para establecer todas aquellas políticas y objetivos de seguridad a través de la implementación de controles de seguridad de la información que los coordine e integre efectivamente, sustentado en el estándar ISO/IEC 27002:2013.

Sin embargo y pese a los esfuerzos de la gerencia, algunos de los empleados de la entidad no han tomado conciencia de la importancia de asegurar la información con la que trabajan (Gerente en conversaciones previas a la viabilidad), bien sea porque desconocen la magnitud del impacto que generaría su pérdida, o bien, porque el nivel de compromiso con la entidad es bajo. Es por ello, que una guía de aplicabilidad de controles de seguridad para la IPS KARISALUD Ltda., de acuerdo con el estándar en mención, permitirá la adopción de buenas prácticas en cuanto a la gestión de la seguridad de la información.

Con el diseño de la guía de aplicabilidad de controles de seguridad propuesta para la IPS KARISALUD Ltda., de acuerdo con el estándar ISO/IEC 27002:2013, se busca mejorar los índices de confidencialidad, integridad y disponibilidad de los datos necesarios para llevar a cabo los procesos de la entidad, de tal manera que los usuarios puedan acceder a información confiable y que el impacto económico para la entidad en cuanto a pérdida o alteración de información, sea mínimo.

Además, dicha guía le permitirá a la IPS contar con la información necesaria en torno a las funciones y el compromiso que deben tener los niveles estratégico, ejecutivo y operativo, en cuanto a la administración de la seguridad de la información.

1.5. Delimitaciones

1.5.1. Geográfica. La presente propuesta de diseño de una guía de aplicabilidad de controles de seguridad para la IPS KARISALUD Ltda., de acuerdo con el estándar ISO/IEC 27002:2013, se desarrolló en la sede principal de la IPS en mención, ubicada en el municipio de Ábrego, Norte de Santander.

1.5.2. Temporal. La presente propuesta se desarrolló en un tiempo de diez (10) semanas, a partir de la fecha de su aprobación.

1.5.3. Conceptual. El marco conceptual del presente proyecto abordó los siguientes desarrollos conceptuales:

Análisis de riesgos, Seguridad informática, Seguridad de la información, Sistema de Gestión de Seguridad de la Información, Declaración de Aplicabilidad.

1.5.4. Operativa. Para el desarrollo del proyecto propuesto, se llevarán a cabo las siguientes acciones:

En primer lugar, se realizará un diagnóstico de la situación actual del manejo de la información en la IPS KARISALUD Ltda., y de la manera como se viene gestionando, a través de una auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013.

En segundo lugar, se realizará un análisis de riesgos de los recursos informáticos y de información de la IPS KARISALUD LTDA.

Finalmente, se elaborará la guía propuesta sobre aplicabilidad de controles de seguridad de acuerdo con el estándar ISO/IEC 27002:2013, en la IPS KARISALUD Ltda.

Capítulo 2. Marco Referencial

2.1. Marco Histórico

2.1.1. Antecedentes a nivel internacional sobre la aplicabilidad del estándar ISO/IEC 27002:2013.

Por medio de revisiones documentales de fuentes digitales, se constató que a nivel internacional existen diferentes propuestas sobre la aplicabilidad del estándar ISO/IEC 27002:2013. Dentro de las que se pueden citar:

(Rojas, 2014) Propone un Plan de Implementación de la ISO / IEC 27001:2013. La autora afirma que con la importante presencia de las Tecnologías de la Información y la Comunicación dentro de las organizaciones y el creciente volumen que se maneja dentro de las empresas, sumado a la tendencia –cada vez más persistente- de estar interconectado, las organizaciones se ven expuestas a una cantidad de retos y amenazas que son cada vez más sofisticadas y que les obliga a proteger la información por ser uno de sus activos más valiosos. Esto ha obligado, según la autora, a que las empresas adopten sistemas para gestionar la seguridad de la información, los cuales deberían ser adecuados a los estándares internacionales. De estos estándares, se pueden destacar la ISO/IEC 27001:2013 e ISO/IEC 27002:2013, que ofrecen una guía de objetivos y controles que permiten –de una manera práctica- la implantación de un sistema que gestione la seguridad de la información de una forma adecuada y acorde con los objetivos de negocio de la empresa.

El Instituto Nacional de Transparencia (2015), IFAI, Acceso a la Información y Protección de Datos Personales, recomendó la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), para la protección de los datos personales (nstituto Nacional de Transparencia, 2015).

La guía, se brinda orientación para la implementación de un SGSDP con base en los siguientes estándares internacionales:

- BS 10012:2009 Data protection – Specification for a personal information management system
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.
- ISO/IEC 27005:2008, Information Technology–Security techniques– Information security risk management.
- ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework
- ISO 31000:2009, Risk management – Principles and guidelines
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards
- ISO GUIDE 73, Risk management – Vocabulary

- ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Con objeto de facilitar el análisis de las normas y estándares anteriores, el IFAI ofrece, a través de la guía, un ejercicio de concreción, síntesis y armonización de dichas referencias. Su objetivo es orientar a los responsables y encargados para crear un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), de manera que a través de un proceso de mejora continua se logre un nivel aceptable del riesgo en el tratamiento de la información personal, de acuerdo al modelo y objetivos de la organización.

Es importante que se tome en cuenta que el alcance del SGSDP es la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Por lo cual, el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de la presente guía se deberán enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Esta guía se basa en la seguridad a través de la gestión del riesgo de los datos personales, entendiéndose de forma general al riesgo como una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo

en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

2.1.2. Antecedentes a nivel nacional sobre sobre la aplicabilidad del estándar ISO/IEC 27002:2013. Por medio de revisiones documentales de fuentes digitales, se constató que a nivel nacional existen diferentes propuestas sobre la aplicabilidad del estándar ISO/IEC 27002:2013. Dentro de las que se pueden citar:

(Santamaria, 2014), Profesional en Comercio Internacional, Universidad Militar Nueva Granada, Bogotá, Colombia, propone un "Manual de seguridad de la información para un organismo del estado colombiano", sustentado en el estándar ISO 27002:2013. El manual de seguridad de la información diseñado permite determinar las fortalezas y debilidades que tiene la organización frente a los activos de información, conocer el estado actual ante seguridad de información y sus controles, con el fin de crear estrategias que minimicen las amenazas que impactan la vulnerabilidad organizacional. La creación de políticas pertinentes y aplicables, basadas en el análisis y evaluación de riesgo de las informaciones obtenidas de los activos que son permitidas valorar, es el resultado de la investigación realizada a la organización.

El método utilizado en este proyecto fue el descriptivo – documental, cuya fuente de información fueron las personas vinculadas a los procesos, las leyes, decretos, resoluciones y normas, a través de técnicas de observación sistemática que permitieron cuantificar las variables

de interés, permitiendo determinar el estado del sistema de información de la empresa objeto, identificando sus factores más relevantes.

(Avendaño, 2015), proponen en su proyecto de grado titulado "Diseño de un modelo de análisis y diagnóstico del nivel de madurez en si para en Mipymes de asesoría legal y oficinas de abogados, como base para la implementación de la norma iso27002" para optar al título de Especialista en Seguridad de la Información. El proyecto consistió en el diseño de metodologías para identificar el nivel de madurez considerando los dominios y objetivos de control de la ISO 27002, identificar y clasificar activos de información, analizar y evaluar riesgos con el propósito de brindarles a las Mipymes de asesoría legal un acercamiento a la seguridad y protección de la información desde diferentes frentes.

El diseño metodológico consistió en el análisis sistemático teniendo en cuenta los componentes más significativos a la hora de fortalecer la Seguridad de la información, a saber:

- Metodología de diagnóstico basada en la norma ISO 27002.
- Metodología para identificación y clasificación de activos de información.
- Metodología de análisis y evaluación de riesgos de activos de información críticos.
- Análisis experto: diseño de controles y recomendaciones.

2.1.3. Antecedentes a nivel local sobre sobre la aplicabilidad del estándar ISO/IEC 27002:2013. Por medio de revisiones documentales de fuentes digitales, se constató que a nivel

local existen diferentes propuestas sobre la aplicabilidad del estándar ISO/IEC 27002:2013. Dentro de las que se pueden citar:

Gerardo Mosquera Quintero, Jorge Armando Saravia Alvernia y José Julián Pacheco Pérez, proponen, para optar al título de Especialista en Auditoría de Sistemas, en la Universidad Francisco de paula Santander Ocaña, un proyecto de grado titulado "Elaboración de políticas de seguridad física y ambiental basados en el estándar internacional ISO/IEC 27002:2013 en el hospital regional José David Padilla Villafañe – ESE, de la ciudad de Aguachica Cesar" (Pacheco, 2013)

El trabajo tuvo por objetivo la creación de las políticas de seguridad física y ambiental que brinden apoyo a la protección de la información en el Hospital José David Padilla Villafañe de Aguachica, para las mejores prácticas en la custodia de la misma, según los lineamientos del estándar internacional ISO/IEC 27002:2013, y a su vez proporcionar un plan de mejora para la optimización, brindando recomendaciones en forma sencilla y entendible, acerca de cómo mejorar los mecanismos para salvaguardar la información.

La metodología utilizada para la elaboración de este proyecto se basó en la aplicación una auditoria previa y basada en el estándar ISO/IEC 27002:2013, en su dominio “11 Seguridad Física y Ambiental”, para posteriormente estructurar el análisis de riesgos que nos permitió identificar las debilidades y amenazas presentadas por el Hospital y finalmente desarrollar las

políticas.

Arrieta, Sanguino & Lobo Sánchez, proponen, para optar al título de Especialista en Auditoría de Sistemas, en la Universidad Francisco de Paula Santander Ocaña, un proyecto de grado titulado "Diseño de un plan estratégico de tecnologías de información para la Universidad Francisco de Paula Santander Ocaña" (Reyes, 2015).

El plan estratégico de tecnologías de la información diseñado está sustentado en la necesidad de proveer un marco de acción que sirva de estrategia a la Universidad Francisco de Paula Santander Ocaña, para optimizar la gestión de los recursos tecnológicos y su incorporación a todos y cada uno de los procesos administrativos y académicos, para el logro de sus objetivos institucionales.

Dado el propósito del proyecto, se llevó a cabo una investigación cualitativa, la cual permitió comprender y explorar los elementos que intervienen en el diseño del plan estratégico en mención, logrando determinar que ésta pudo ser la mejor opción para optimizar los procesos de la Universidad a través del uso eficiente de las tecnologías de información y comunicación.

2.2. Marco Teórico

La gestión de la seguridad de la información, se ha constituido hoy por hoy en un referente obligado para cualquier organización que quiera garantizar la confiabilidad de los datos que se

derivan de la interacción con sus clientes, toda vez que dicha información se ve constantemente sometida a las amenazas y riesgos por las acciones fraudulentas de enemigos potenciales que buscan apropiarse de ella para beneficio personal o de terceros.

Es por ello que la información ha pasado de ser un aspecto secundario y hoy se le considera como uno de los activos más importantes, o quizá el más importante, dentro de las empresas, tanto públicas como privadas. Cuanto más grandes sean éstas, mayores y complejos deben ser los protocolos que se implementen para salvaguardar la información, traducidos en políticas que garanticen la seguridad física y lógica de la misma, garantizando así la privacidad y la protección de los datos derivados de su interacción con sus clientes y proveedores.

Aunque no existe en la actualidad un sistema de seguridad de la información ciento por ciento seguro, sin embargo, ya existe consenso en torno a las características fundamentales que dichos sistemas deben cumplir: integridad, esto es niveles de acceso a la información; confidencialidad, esto es, garantizar los niveles de reserva para la información sensible; la disponibilidad, es decir, información oportuna y veraz cuando se a requerida; y finalmente, la irrefutabilidad, es decir, la certeza de su autoría. Otro aspecto importante en la gestión de la seguridad de la información, es el hecho de que la empresa pueda garantizar que sus activos informáticos cumplan cabalmente sus propósitos, es decir que no presenten fallas estructurales o sean alterados por circunstancias o factores externos.

En este orden de ideas, puede entenderse entonces la seguridad como el conjunto de protocolos y procedimientos técnicos implementados para prevenir, proteger y resguardar los activos físicos y lógicos relacionados con la gestión de la información, que sean susceptibles de robo, perdida o daño, ya sea de manera individual, colectivo o empresarial; para ello, dichos protocolos y procedimientos deben garantizar que la información sea protegida, resguardada y recuperada sin daños considerables ni pérdidas lamentables.

La seguridad de la información es quizá el elemento clave en el éxito de toda organización, por lo que es de obligatorio cumplimiento, la implementación de políticas que la garanticen y que orienten internamente a dicha organización, a fin de que pueda evidenciar procedimientos y reglas para la interacción entre sus activos, los usuarios y la información que se derive de la misma. Para que esto sea posible, es necesario que cada organización diseñe e implemente sus sistemas para la gestión de la seguridad de la información, con base en los estándares y normas que para el efecto se han acordado internacionalmente.

2.3. Marco Conceptual

2.3.1. Seguridad informática. La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad (acceso autenticado y controlado), integridad (datos completos y non-modificados) y disponibilidad (acceso garantizado) (www.protejete.wordpress.com, 2015).

Considerar aspectos de seguridad significa a) conocer el peligro, b) clasificarlo y c) protegerse de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos.

En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

2.3.2. Gestión de Riesgos en la Seguridad Informática.. La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo (www.protejete.wordpress.com, s.f.).

En su forma general contiene cuatro fases

Análisis. Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

Clasificación. Determina si los riesgos encontrados y los riesgos restantes son aceptables.

Reducción. Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

Control. Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

2.3.3. Seguridad de la Información y Protección de Datos. En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos (www.protejete.wordpress.com, 2015).

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección. Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la

Información y la Protección de Datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otros consecuencias negativas para la institución.

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta. Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, sí o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

2.3.4. Retos de la Seguridad. La eficiente integración de los aspectos de la Seguridad Informática en el ámbito de las organizaciones sociales centroamericanas enfrenta algunos retos muy comunes que están relacionados con el funcionamiento y las características de estas (www.protejete.wordpress.com, 2015).

Los temas transversales no reciben la atención que merecen y muchas veces quedan completamente fuera de las consideraciones organizativas: Para todas las organizaciones y empresas, la propia Seguridad Informática no es un fin, sino un tema transversal que normalmente forma parte de la estructura interna de apoyo. Nadie vive o trabaja para su seguridad, sino la implementa para cumplir sus objetivos:

- Carencia o mal manejo de tiempo y dinero, es decir, implementar medidas de protección significa invertir en recursos como tiempo y dinero.
- El proceso de monitoreo y evaluación, para dar seguimiento a los planes operativos está deficiente y no integrado en estos, es decir, implementar procesos y medidas de protección, para garantizar la seguridad, no es una cosa que se hace una vez y después se olvide, sino requiere un control continuo de cumplimiento, funcionalidad y una adaptación periódica, de las medidas de protección implementadas, al entorno cambiante.

Todas estas circunstancias juntas, terminan en la triste realidad, que la seguridad en general y la Seguridad Informática en particular no recibe la atención adecuada. El error más común que se comete es que no se implementa medidas de protección, hasta que después del desastre, y las escusas o razones del porque no se hizo/hace nada al respecto abundan.

Enfrentarse con esta realidad y evitando o reduciendo los daños a un nivel aceptable, lo hace necesario trabajar en la “Gestión de riesgo“, es decir conocer el peligro, clasificarlo y protegerse de los impactos o daños de la mejor manera posible.

Pero una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios y que requiere el reconocimiento y apoyo de las directiva. Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

2.3.5. Elementos de Información. (Markus, 2015) Los elementos de información son todos los componentes que contienen, mantienen o guardan información. Dependiendo de la literatura, también son llamados activos o recursos.

Son estos los Activos de una institución que tenemos que proteger, para evitar su perdida, modificación o el uso inadecuado de su contenido, para impedir daños para nuestra institución y las personas presentes en la información.

Generalmente se distingue y divide tres grupos:

- Datos e Información: son los datos e informaciones en sí mismo.
- Sistemas e Infraestructura: son los componentes donde se mantienen o guardan los datos e informaciones.
- Personal: son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles.

2.3.6. Amenazas y Vulnerabilidades. (Markus, Gestión de riesgo en la seguridad informática, 2015) Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos. Generalmente se distingue y divide tres grupos:

- Criminalidad: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- Sucesos de origen físico: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las

amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

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. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política.

2.3.7. Análisis de Riesgo. (Erb, 2015) El primer paso en la Gestión de 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.

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación.

Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quiénes tienen acceso a qué información y datos.

Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quiénes tienen acceso a qué datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado. Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo. La valoración del riesgo basada en la fórmula matemática

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4). En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo facilita el uso de herramientas técnicas como hojas de cálculo.

Nota: La escala (4 condiciones) de la Probabilidad de Amenaza y Magnitud de Daño no es fijo y puede ser adaptada y afinada a las necesidades propias. En diferentes literaturas, particularmente la Probabilidad de Amenaza puede tomar hasta seis diferentes condiciones.

Como se mencionó, el reto en la aplicación del método es precisar o estimar las condiciones (valores) de las dos variables, porque no basen en parámetros claramente medibles. Sin embargo, el análisis de riesgo nos permite ubicar el riesgo y conocer los factores que influyen, negativa- o positivamente, en el riesgo.

En el proceso de analizar un riesgo también es importante de reconocer que cada riesgo tiene sus características:

- Dinámico y cambiante (Interacción de Amenazas y Vulnerabilidad).
- Diferenciado y tiene diferentes caracteres (caracteres de Vulnerabilidad).

No siempre es percibido de igual manera entre los miembros de una institución que tal vez puede terminar en resultados inadecuados y por tanto es importante que participan las personas especialistas de los diferentes elementos del sistema (Coordinación, Administración financiera, Técnicos, Conserje, Soporte técnico externo etc.)

El modelo se pude aplicar a los diferentes elementos de manera aislada, sino también a los sistemas completos, aunque en el primer caso, el resultado final será más preciso pero también requiere más esfuerzo.

Mientras más alta la Probabilidad de Amenaza y Magnitud de Daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar medidas de protección.

2.3.7.1. Probabilidad de amenaza. Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicado respecto a su confidencialidad, integridad, disponibilidad y autenticidad.

Para estimar la Probabilidad de Amenaza se pueden plantear algunas preguntas:

¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos? ¿Cuáles son nuestras vulnerabilidades? ¿Cuántas veces ya han tratado de atacarnos?

Considerando todos los puntos anteriores, se puede clasificar la Probabilidad de Amenaza. Sin embargo, antes tenemos que definir el significado de cada condición de la probabilidad (Baja, Mediana, Alta). Las definiciones mostradas en la imagen anterior solo son un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propias condiciones.

2.3.7.2. Magnitud de Daño. Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso.

Aunque conozcamos bien el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde manejamos la información, sea en una ONG (derechos humanos, centro de información etc.), en una empresa privada (banco, clínica, producción etc.), en una institución Estatal o en el ámbito privado. Otro factor decisivo, respecto a las consecuencias, es también el entorno donde nos ubicamos, es decir cuáles son las Leyes y prácticas comunes, culturales que se aplica para sancionar el incumplimiento de las normas.

Un punto muy esencial en el análisis de las consecuencias es la diferenciación entre los dos propósitos de protección de la Seguridad Informática, la Seguridad de la Información y la Protección de datos, porque nos permite determinar, quien va a sufrir el daño de un impacto, nosotros, otros o ambos. En todo caso, todos nuestros comportamientos y decisiones deben ser dirigidos por una conciencia responsable, de no causar daño a otros, aunque su realidad no tenga consecuencias negativas.

Otras preguntas que podemos hacernos para identificar posibles consecuencias negativas causadas por un impacto son:

¿Existen condiciones de incumplimiento de confidencialidad (interna y externa)? ¿Existen condiciones de incumplimiento de obligación jurídicas, contratos y convenios? ¿Cuál es el costo de recuperación?

Considerando todos los aspectos mencionados, nos permite clasificar la Magnitud del Daño. Sin embargo, otra vez tenemos que definir primero el significado de cada nivel de daño (Baja, Mediana, Alta).

Las definiciones mostradas en la imagen anterior solo son un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propios niveles.

2.3.8. Sistema de Gestión (Informacion, 2010)**.** Un Sistema de Gestión implementa los procesos que permiten que una Un Sistema de Gestión implementa los procesos que permiten que una Organización realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales.

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

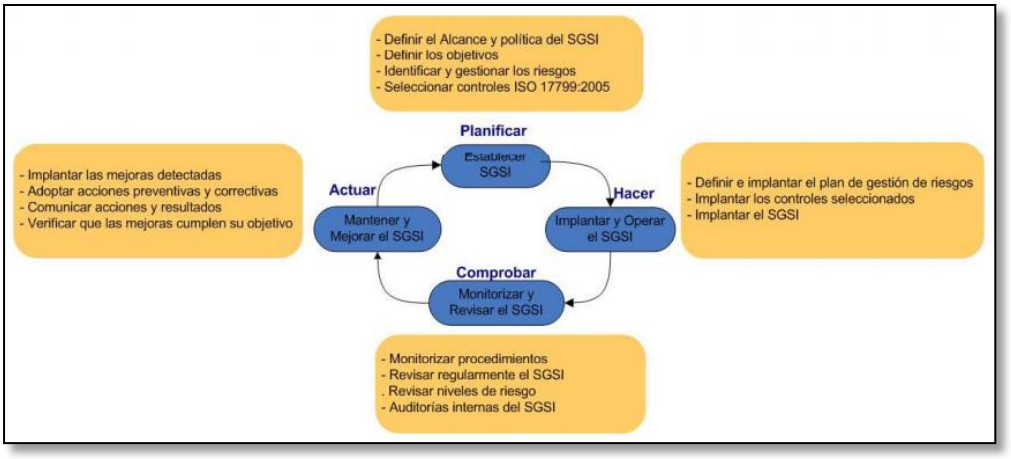

Figura 1. *Implementación de un SGSI.*
Nota Fuente: http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

2.3.8.1. Normas y estándares de Implantación de un Sistema de Gestión de Seguridad de la Información. Para la implantación de un SGSI se consideran:

- La norma ISO/IEC 27001:2005: "Especificaciones para los Sistemas de Gestión de la Seguridad de la Información", requeridas para obtener la certificación del SGSI implantado.

- El estándar ISO/IEC 27002, “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. Estructurada en 11 dominios desglosados a su vez en 133 controles, que cubren todos los aspectos fundamentales de la seguridad en el tratamiento de la información.

2.3.8.2. Utilidad de un Sistema de Gestión de Seguridad de la Información. Con un Sistema de Gestión de Seguridad de la Información, 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 actualiza constantemente.

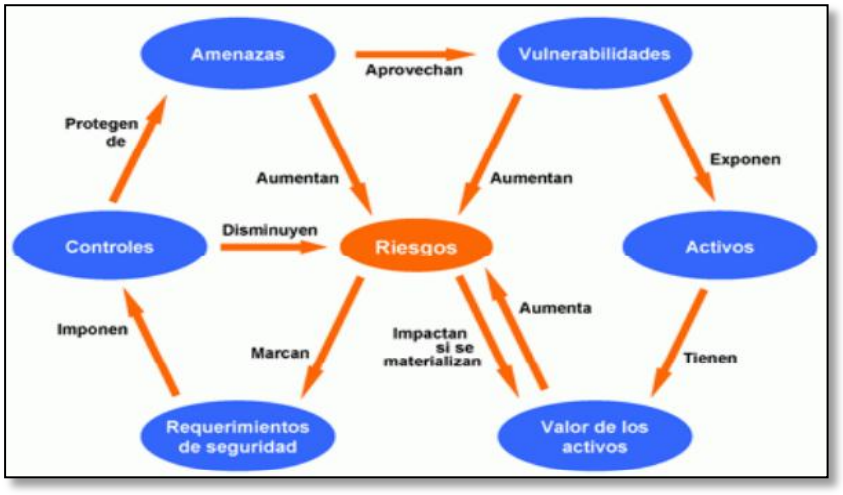

Figura 2. *Utilidad de un SGSI.*
Nota Fuente: http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

2.3.9. Declaración de aplicabilidad (Mendoza, 2015)- Se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).

Los propósitos que se desean alcanzar a través de la implementación de controles (es decir, objetivos de control), se encuentran incluidos de manera implícita en los controles seleccionados.

Sin embargo, es importante mencionar que un Sistema de Gestión de Seguridad de la Información no está limitado a los que se encuentran listados en el anexo, por lo cual pueden ser utilizados otros controles y objetivos de control si se considera necesario.

La Declaración de Aplicabilidad se desarrolla luego del tratamiento de riesgos, que a su vez es la actividad posterior a una evaluación de riesgos. El tratamiento tiene como objetivo la definición de las acciones a realizar para mitigar aquellos riesgos que han sido identificados y analizados. Existen varias opciones de tratamiento, aunque de manera general se pueden agrupar en las siguientes categorías:

- **Mitigar**. Consiste en implementar algún control que reduzca el riesgo.
- **Transferir**. Ocurre cuando se delega la acción de mitigación a un tercero.

- **Aceptar**. Se presenta cuando el impacto generado por un riesgo es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo.

Una vez que se han definido las opciones de tratamiento para los riesgos, la organización debe aplicar medidas de seguridad, es decir, decidir de qué manera serán mitigados los riesgos. Es en este punto cuando se desarrolla un Sistema de Gestión de Seguridad de la Información, el documento donde se registran los controles de seguridad que son aplicables (necesarios) y si éstos se encuentran operando o todavía no.

En una declaración de aplicabilidad puede encontrarse en el formato que más convenga a una organización; lo relevante es su contenido, que en general debe incluir los objetivos de control y controles seleccionados del estándar, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso.

También, debe indicar si los objetivos de control y controles se encuentran implementados y operando, los que hayan sido descartados, así como una justificación del porqué algunas medidas han sido excluidas (las que son innecesarias y la razón del porqué no son requeridas en una organización).

Los controles indicados en la Declaración de Aplicabilidad pueden ser seleccionados debido a distintas razones, por ejemplo, como resultado de una evaluación de riesgos, si se debe

cumplir con algún requisito legal, obligaciones adquiridas por contratos o regulaciones, nuevos requisitos del negocio, mejores prácticas a utilizar, entre otras.

Posteriormente, la selección de controles de seguridad deriva en la creación de un plan de tratamiento de riesgos, principalmente para la definición de las actividades necesarias para la aplicación de los controles de seguridad, que hayan sido seleccionados y que no se encuentran implementados.

2.4. Marco Legal

DOCUMENTO CONPES 3072 AGENDA DE CONECTIVIDAD 9 DE FEBRERO DE 2000. A través del cual se presenta a consideración del CONPES la "Agenda de Conectividad", que busca masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002 "Cambio para Construir la Paz".

PLAN NACIONAL DE TIC 2008- 2019. Busca que, al final de este período, todos los colombianos se informen y se comuniquen haciendo uso eficiente y productivo de las Tecnologías de Información y Comunicación TIC, para mejorar la inclusión social y aumentar la competitividad. Para lograr este objetivo se proponen una serie de políticas, acciones y proyectos en ocho ejes principales, cuatro transversales y cuatro verticales. Los ejes transversales cubren

aspectos y programas que tienen impacto sobre los distintos sectores y grupos de la sociedad. Los ejes verticales se refieren a programas que harán que se logre una mejor apropiación y uso de las TIC en sectores considerados prioritarios para este Plan.

Los ejes transversales son:

- Comunidad.
- Marco regulatorio.
- Investigación, Desarrollo e Innovación.
- Gobierno en Línea.

Los cuatro ejes verticales son:

- Educación.
- Salud.
- Justicia.
- Competitividad Empresarial.

LEY 72 DEL 20 DE DICIEMBRE DE 1989. El Gobierno Nacional, por medio del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios de dicho sector, que comprende, entre otros:

- Los servicios de telecomunicaciones.
- Los servicios informáticos y de telemática.
- Los servicios especializados de telecomunicaciones o servicios de valor agregado.
- Los servicios postales.

LEY 555 DEL 2 DE FEBRERO DE 2000 EN LA LEY NO. 1341 DEL 30 DE JULIO DE 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.", muestra el esfuerzo que ha tenido el gobierno colombiano por brindar un marco normativo para el desarrollo de tecnologías de la información y la comunicación.

Artículo 2o. Principios orientadores. Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente ley:

Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de

bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad.

Artículo 3o. Sociedad de la Información y del Conocimiento.

El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Norma ISO/IEC 27001 (Ruiz, 2014). Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, entre ellos:

- Norma ISO/IEC 27001: Define los requisitos para la implementación de un
- SGSI (Sistema de Gestión de la Seguridad de la Información).
- Norma ISO/IEC 27002: (anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.

- Norma ISO/IEC 27003: Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.
- Norma ISO/IEC 27004: Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.
- Norma ISO/IEC 27005: Suministra directrices para la gestión del riesgo en la seguridad de la información.

Ley 1273 de 2009: sobre los delitos informáticos y la protección de la información y de datos en Colombia.

Capítulo 3. Diseño Metodológico

3.1. Tipo de Investigación

Dada la naturaleza del presente proyecto, se llevará a cabo una investigación cuantitativa, puesto que la misma, permitirá comprender las características de los elementos que participan en el diseño de una guía de aplicabilidad de controles de seguridad para la IPS KARISALUD Ltda., de acuerdo con el estándar ISO/IEC 27002:2013, definiéndola como la mejor opción para proponer controles para una adecuada administración de la seguridad de la información.

3.2. Población y muestra

Para el presente proyecto, se tomará como población a los responsables de las siguientes dependencias, por dirigir procesos relacionados con la gestión de la seguridad de la información en la IPS KARISALUD Ltda.: *Gerente y Jefe de personal.* La muestra estará representada por el 100% de la población.

3.3. Técnicas e instrumentos de recolección de información

En el diseño de la guía de aplicabilidad de controles de seguridad para la IPS KARISALUD Ltda., de acuerdo con el estándar ISO/IEC 27002:2013, en primera instancia se utilizará, como técnica de recolección de información la entrevista y como instrumento un cuestionario que será aplicado a la población mencionada anteriormente, con el fin de realizar un

diagnóstico de la manera como se ha gestionado la seguridad de la información en la IPS (Ver Anexos A y B).

Capítulo 4. Resultados

4.1. Diagnóstico de la seguridad informática y de la información en KARISALUD IPS LTDA.

Con el fin de realizar un análisis de la situación actual en cuanto a seguridad informática y de la información en KARISALUD IPS LTDA., se llevó a cabo una evaluación de cumplimiento de los dominios, objetivos de control y controles contemplados en el estándar ISO/IEC 27002:2013.

Las áreas evaluadas por tener relación con los dominios de la Norma, fueron: Gerencia, Historias Clínicas y Auditoría.

Los resultados de la evaluación aplicada, se presentan a continuación, de acuerdo con la siguiente estructura:

4.1.1. Aspectos generales de la empresa auditada. KARISALUD IPS LTDA., se creó en acuerdo y en concordancia con el Decreto Departamental Nº 2309/02 del 02 de enero del 2006. La sede principal se encuentra ubicada en Colombia en la parte Sur Occidente del Municipio de Ábrego desde el 2008 y su respectiva sede de apoyo ubicada en Ocaña, municipio ubicado en área de fácil acceso del Departamento de Norte de Santander.

KARISALUD IPS LTDA. Tiene como actividad principal la práctica médica sin internación, actividad secundaria, apoyo diagnóstico y actividad adicional, comercio al por menor de productos farmacéuticos y medicinales, cosméticos y artículos de tocador en establecimientos especializados. Constituye afiliados de régimen subsidiado y contributivo, los dos tipos de regímenes dispuestos bajo las normas del Estado Colombiano para la adscripción y atención a un modelo de salud de la población en el país.

Las funciones de KARISALUD IPS LTDA., para estos dos tipos de afiliados se basan en asesorar, administrar, elaborar, ejecutar y vigilar los servicios habilitados en el área de la salud incluyendo acciones de detección temprana y protección específica, acciones asistenciales y preventivas de baja y mediana complejidad enfocadas a grupos especiales, susceptibles de morbimortalidad.

Los servicios ofertados de baja y mediana complejidad por KARISALUD IPS son: medicina general, odontología general, promoción y prevención, toma de muestra y laboratorio clínico, nutrición, psicología, terapia respiratoria, fisioterapia, terapia ocupacional, fonoaudiología y especializado en los siguientes campos: medicina interna, gineco-obstetricia, pediatría, cirugía general y ortopedia y/o traumatología.

Misión

Es una Institución prestadora de servicios en salud, orientada a contribuir con el mejoramiento de la calidad de vida de nuestros usuarios, que cuenta con profesionales idóneos y comprometidos, que trabajan de manera permanente con eficiencia, responsabilidad y calidez humana, ofreciendo así, un alto sentido de responsabilidad social.

Visión

KARISALUD IPS LTDA en el año 2020 será líder en primer nivel en la región, reconocida por sus altos estándares de calidad, excelencia en la atención, grandes profesionales trabajando en equipo, y con una infraestructura que brinde un ambiente agradable, que satisfaga las expectativas de nuestros usuarios y de esta manera aportar nuestro granito de arena, para que esta sociedad cada día sea mejor.

Estructura Organizacional

La estructura organizacional de KARISALUD IPS LTDA, permite desarrollar las funciones necesarias para otorgar los servicios de salud con los que están comprometidos, lo que se puede apreciar en la Figura 3 que se presenta a continuación.

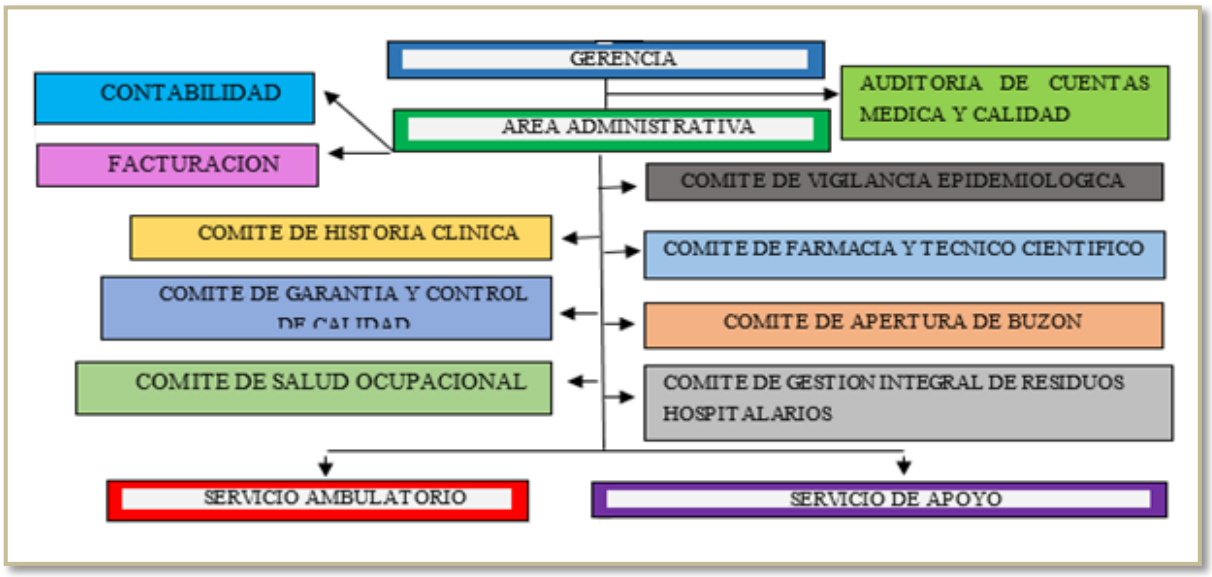

Figura 3. Organigrama KARISALUD IPS.

Nota Fuente: KARISALUD IPS.

4.1.2. Aspectos de la auditoría

4.1.2.1. Objetivo General. Evaluar el grado de cumplimiento de las actividades relacionadas con la seguridad de la información en KARISALUD IPS LTDA., de acuerdo con lo estipulado en el estándar ISO 27002:2013

4.1.2.2. Alcances. Para llevar a cabo la auditoría de cumplimiento, se hizo necesario evaluar la existencia y eficiencia de los controles contemplados en el estándar ISO/IEC 27002:2013 para KARISALUD IPS LTDA., del municipio de Ocaña, Norte de Santander, en lo relacionado con la gestión de la seguridad de la información.

La auditoría realizada incluyó la evaluación de los siguientes dominios:

- Dominio 5: Políticas de Seguridad
- Dominio 6: Aspectos organizativos de la seguridad de la información
- Dominio 7: Seguridad ligada a los recursos humanos
- Dominio 8: Gestión de activos
- Dominio 9: Control de accesos
- Dominio 10: Cifrado
- Dominio 11: Seguridad física y ambiental
- Dominio 12: Seguridad en la operativa. Sólo se evaluaron los objetivos de control:

    - *Protección contra código malicioso*
    - *Copias de seguridad*

- Dominio 13: Seguridad en las telecomunicaciones
- Dominio 14: Sólo se evaluó el objetivo de control:

    - *Requisitos de seguridad de los sistemas de información*

- Dominio 15: Relaciones con los suministradores
- Dominio 16: Gestión de incidentes en la seguridad de la información
- Dominio 17: Aspectos de seguridad de la información en la gestión de la continuidad del negocio

- Dominio 18: Cumplimiento

Los objetivos de control que no se tuvieron en cuenta, no aplican para la evaluación, debido a que la IPS en mención, a pesar de que utiliza aplicaciones de software para algunos de sus procesos, no produce o desarrolla software.

4.1.2.3. Metodología. Para llevar a cabo la auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013 a las áreas que tienen que ver con los procesos de gestión de seguridad de la información en KARISALUD IPS LTDA., se organizaron las siguientes actividades:

Solicitud de documentación. Para dar cumplimiento a esta actividad, se presentó un oficio a la Gerente de KARISALUD IPS LTDA., mediante el cual, se hizo la solicitud de la siguiente documentación, necesaria para realizar el estudio inicial del entorno a auditar:

- *Reseña de la IPS*
- *Horizonte institucional (misión, visión, objetivos, políticas de calidad)*
- *Políticas de seguridad de la información*
- *Manual de funciones*
- *Manual de procedimientos*
- *Plan de contingencias*
- *Características de la red de datos*
- *Manual de usuario de las aplicaciones*
- *Inventario de hardware y software*

Definición de objetivos y actividades de auditoría. Se diseñó el formato de programa de auditoría (Ver Cuadro 1), que contempla las acciones necesarias para la realización de la auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013.

Diseño de instrumentos de recolección de información. Se hizo necesario diseñar una serie de herramientas en las que se pudiera hacer la recolección de la información útil para obtener el diagnóstico y que éste, pudiera ser lo más objetivo y cercano a la realidad de la IPS en estudio. Los formatos de entrevistas, listas de chequeo y demás, se encuentran como anexos de este documento.

Ejecución de las actividades de auditoría. Una vez se diseñaron los instrumentos, se comenzó el proceso de aplicación de los mismos. Cabe destacar, que esta tarea, no en todos los casos fue exitosa, debido a los altos compromisos de las personas focalizadas para las entrevistas y listas de chequeo. De la misma forma, la información que no se obtuvo a partir de la documentación inicial, tuvo que ser recolectada posteriormente, dando lugar a la reformulación de algunos de los instrumentos previamente diseñados.

Redacción de los hallazgos de la auditoría. Los resultados de la auditoría de cumplimiento y que se utilizará como diagnóstico, se presenta en la sección de Hallazgos de la Auditoría.

Cuadro 1. *Programa de auditoría.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

PROGRAMA DE AUDITORÍA

R/PT PA001

Empresa: **KARISALUD IPS LTDA** Área o Proceso**: Seguridad de la Información**	Fecha Inicio: 12/05/2016 Fecha Final: 22/07/2016

Auditor Principal: **Jean Carlos García Guarín**
Auditora Junior: **Dina Luz Orozco Cantillo**

OBJETIVO GENERAL:
Evaluar el grado de cumplimiento de las actividades relacionadas con la seguridad de la información en KARISALUD IPS LTDA., de acuerdo con lo estipulado en el estándar ISO 27002:2013

OBJETIVOS ESPECÍFICOS:
1. Evaluar la implementación y documentación de los controles relacionados con la seguridad de la información en lo que respecta a los dominios: 5, 6, 9, 12, 13, 14, 15, 16 y 17 del estándar ISO/IEC 27002 de 2013.
2. Comprobar la existencia y eficiencia de procedimientos relacionados con la seguridad de la información ligada a los recursos humanos de KARISALUD IPS LTDA, en cada una de los momentos del proceso de contratación de personal (antes, durante y después de la contratación), de acuerdo como lo establece el estándar ISO/IEC 27002 de 2013.
3. Evaluar los controles relacionados con la protección de los activos de información de KARISALUD IPS LTDA.
4. Revisar la existencia y eficacia de los controles relacionados con la seguridad física y ambiental en KARISALUD IPS LTDA.
5. Evaluar el grado de conformidad de los requisitos legales y estándares de seguridad de KARISALUD IPS, relacionados con el dominio de Cumplimiento de acuerdo con lo estipulado en el estándar ISO 27002:2013

Alcances
La presente auditoría pretende evaluar todos los dominios del estándar ISO/IEC 27002:2013, en cuanto a requerimientos de seguridad de la información. Se especificarán aquellos objetivos de control que por la naturaleza de la organización, no apliquen para tal auditoría.

ÍTEM	ACTIVIDAD	AUDITADO	R/PT
1.1	Evaluar el grado de cumplimiento de las actividades relacionadas con la seguridad de la información, de acuerdo con lo establecido en el estándar ISO 27002:2013, en sus dominios 5, 6, 9, 12, 13, 14, 15, 16 y 17.	GERENTE	EN001
1.2	Verificar la implementación de los controles relacionados con la protección de la información.	EMPLEADO	EN005
1.3	Verificar la existencia de controles para la gestión de la continuidad del negocio en KARISALUD IPS LTDA.	GERENTE	LC004
2.1	Evaluar el grado de cumplimiento de KARISALUD IPS en relación con el dominio de Seguridad ligada a los Recursos Humanos, contemplado en el estándar ISO 27002:2013.	GERENTE	EN002
3.1	Evaluar el grado de cumplimiento de KARISALUD IPS en relación con el dominio de Gestión de Activos, específicamente en el manejo de las historias clínicas, de acuerdo con lo estipulado en el estándar ISO 27002:2013	ENCARGADO HISTORIAS CLÍNICAS	EN003
3.2	Evaluar la existencia de procedimientos establecidos por KARISALUD IPS, para la protección de sus activos de información.	GERENTE	LC003

Fuente: *Elaboración propia.*

Cuadro 1. *Continuación.*

4.1	Evaluar la existencia de controles de acceso físico a las instalaciones de KARISALUD IPS.	GERENTE	LC001
4.2	Evaluar la existencia y eficacia de los controles para la protección de los equipos de cómputo.	GERENTE	LC002
5.1	Evaluar el cumplimiento de los requisitos legales en cuanto a seguridad de la información en KARISALUD IPS LTDA.	GERENTE – AUDITOR	EN004
MARCAS UTILIZADAS			
PA001: Programa de Auditoría # 1 EN001: Entrevista # 1 EN002: Entrevista # 2 EN003: Entrevista # 3 EN004: Entrevista # 4 EN005: Entrevista # 5 LC001: Lista de verificación # 1 LC002: Lista de verificación # 2 LC003: Lista de verificación # 3 LC004: Lista de verificación # 4			

Nota Fuente*: Elaboración propia.*

4.2.1.4. Hallazgos de la auditoría. A continuación se presentan los hallazgos de la evaluación, por cada dominio del estándar ISO/IEC 27002:2013:

DOMINIO 5: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

KARISALUD IPS LTDA, en la actualidad no posee ningún documento de políticas de seguridad, que contenga los lineamientos específicos para el aseguramiento de la información y para el uso adecuado de los demás activos informáticos de la empresa.

DOMINIO 6: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

En lo que tiene que ver con la organización de la seguridad de la información, la IPS en estudio no cuenta con un marco regulatorio para establecer los procedimientos de adopción e implementación de los controles necesarios para la seguridad de la información que produce y utiliza en cada uno de sus procesos (estratégicos, misionales y de soporte); por lo tanto, no existen responsabilidades claramente definidas para la protección de los activos individuales, ni mucho menos una política de segregación de funciones.

De la misma manera, KARISALUD IPS LTDA, no posee procedimientos formales para establecer contacto con autoridades relevantes para los casos en los que se presente un incidente de seguridad que pueda poner en riesgo los servicios que ofrece la Institución.

DOMINIO 7: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

En el proceso de reclutamiento de personal, la IPS a través de la gerente, (cabe resaltar, que no existe un área de Recursos Humanos) realiza la respectiva revisión de los antecedentes y hoja de vida de los aspirantes a un nuevo cargo dentro de la Institución, pero una vez contratado el personal, no se le hace firmar ningún acuerdo de confidencialidad que especifique las responsabilidades frente a la protección de la información que va a utilizar durante su permanencia en la empresa, ni de las sanciones que puede acarrear el uso inadecuado de éste; así mismo no existe ningún procedimiento para el cese o cambio de puesto de trabajo, que especifique qué hacer con la información en cualquiera de los casos.

Por su parte, los empleados reciben capacitación en cuanto a procedimientos de seguridad de la información que tienen bajo su responsabilidad, pero no existe formalmente un plan que así lo estipule.

DOMINIO 8: GESTIÓN DE ACTIVOS

KARISALUD IPS LTDA, administra un inventario de sus activos, estableciendo una clasificación y un propietario para los mismos; sin embargo, no existen procedimientos de seguridad, codificación y etiquetado de los activos; tampoco, políticas de eliminación y administración de activos fuera de la empresa. La Institución no administra de forma correcta el uso de los medios extraíbles de información, por lo que todo el personal tiene acceso a ellos

En lo que respecta a las historias clínicas, para establecer el intercambio de información, se firman acuerdos entre las partes interesadas para tal efecto; cabe resaltar que no existe ningún protocolo establecido que permita definir el nivel de confidencialidad de la información de las historias clínicas de los usuarios de la IPS.

DOMINIO 9: CONTROL DE ACCESOS

La IPS no cuenta con políticas de seguridad de la información, ni procedimientos de control de acceso a los sistemas de información establecidos formalmente. Para el ingreso a las aplicaciones, los empleados poseen un usuario y contraseña, pera esta información no es

actualizada de forma permanente; no se evidencian controles de gestión de acceso de usuarios, ni restricciones de la información confidencial de tales accesos.

Es de anotar que la administración de la información de las aplicaciones utilizadas en la IPS, es responsabilidad de un estudiante de Ingeniería de Sistemas, que brinda sus servicios a la Institución; esta situación puede poner en riesgo la disponibilidad de los servicios que ofrece la IPS, al no contar con una persona de tiempo completo para este tipo de responsabilidades.

DOMINIO 10: CIFRADO

No existe un control para la asignación de privilegios de acceso a los sistemas de información, ni existe procedimiento formal para realizarlo. El proceso de gestión de claves de usuario se lleva a cabo por el administrador del sistema (Estudiante de Ingeniería de Sistemas).

DOMINIO 11: SEGURIDAD FÍSICA Y AMBIENTAL.

En cuanto a áreas seguras, se pudo determinar que existen perímetros de seguridad definidos para algunas de las áreas de mayor criticidad en cuanto a la información que manejan, como es el caso de Archivo, Farmacia y Gerencia.

Existen cámaras de vigilancia tanto en el área administrativa, como en el de Atención al Usuario; sin embargo, por motivos de remodelación de la sede principal, no se han instalado adecuadamente, lo que impide el registro de los accesos a la institución.

Por su parte, para la protección física de los equipos, KARISALUD IPS LTDA., posee una planta eléctrica para darle continuidad a los servicios que ofrece a sus usuarios en los casos en los que el fluido eléctrico sea suspendido de forma temporal; existe independencia y protección del cableado eléctrico y de datos; posee extintores para casos de incendios; pero no cuenta con pararrayos, ni detectores de humo; el sistema de refrigeración de equipos mediante aire acondicionado está pendiente de instalación, al igual que la señalización del tipo de cableado de datos utilizado en las conexiones de los equipos de cómputo. No existen tampoco avisos formales de prohibiciones de fumar o comer en las áreas restringidas.

DOMINIO 12: SEGURIDAD EN LA OPERATIVA

No existen controles para la detección y prevención de la información contra código malicioso o contra cualquier otro evento que pueda poner en riesgo su integridad, disponibilidad y confidencialidad.

Por su parte, en términos de recuperación de la información, los empleados que tienen bajo su responsabilidad el manejo de aplicaciones de software, realizan copias de respaldo de la base de datos en memorias USB, que mantienen permanentemente en su puesto de trabajo. Hasta el

momento, no se ha probado la restauración de dichos respaldos para garantizar que evidentemente, ante un incidente de seguridad, la información pueda restablecerse exitosamente.

DOMINIO 13: SEGURIDAD EN LAS TELECOMUNICACIONES

En cuanto a la seguridad de la red de datos de la IPS, no se tiene instalado un firewall o cortafuegos que impida el tráfico no autorizado desde Internet hacia la red interna y entre los equipos de la misma red, con el fin de evitar accesos no autorizados.

De igual forma, no existen reglas para el uso de la red interna e Internet, control de conexión a la red, acceso a redes sociales, acceso a páginas con contenido específico, etc.

DOMINIO 14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

En cuanto a los requisitos de seguridad de los sistemas de información que se adquieren, no existe un protocolo de revisión de tales requisitos antes de la contratación, ni en el proceso de puesta en producción del sistema; por este motivo, se presentan constantemente problemas en el software instalado y el soporte a usuarios es muy escaso.

Para la adquisición de tecnología de hardware y software, no se realizan proyecciones de los requerimientos en lo que tiene que ver con la ampliación y mejoramiento de la capacidad tecnológica de la IPS.

DOMINIO 15: RELACIONES CON SUMINISTRADORES

Cuando se establecen acuerdos con terceros (contratistas, proveedores, entre otros), la verificación del cumplimiento de los servicios ofrecidos por éstos no se realiza; sólo se hace una solicitud de antecedentes al inicio de la contratación, pero el proceso de entrega y cumplimiento del objeto del contrato, no se lleva a cabo.

DOMINIO 16: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

KARISALUD IPS LTDA., no cuenta con procedimientos formales de reporte de eventos de seguridad que puedan tener un impacto negativo en los activos institucionales. Para los casos en los que se presentan fallas en las aplicaciones, se establece contacto con el estudiante de Ingeniería de Sistemas que presta sus servicios a la IPS como administrador del sistema.

Hasta el momento, no se han presentado casos de fallas en el sistema por ataques externos.

DOMINIO 17: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

En la actualidad, KARISALUD IPS LTDA., no posee un Plan de Continuidad del Negocio, que contemple las actividades necesarias para minimizar el impacto de un incidente de seguridad en la Institución y que le permita recuperarse ante la pérdida parcial o total de información o de otros activos informáticos, hasta un nivel aceptable.

La Institución, no cuenta con pólizas para asegurar los equipos contra pérdida parcial o total, ni posee procedimientos para la verificación y revisión de la seguridad de la información, para los casos en los que se presente un incidente que pueda poner en jaque la prestación de los servicios administrativos y asistenciales.

DOMINIO 18: CUMPLIMIENTO

KARISALUD IPS LTDA., carece de un documento de políticas de seguridad de la información que especifique los lineamientos de seguridad de todos sus activos y de las repercusiones legales de la contravención de tales políticas; no existen controles definidos y documentados para proteger los registros y la información de la IPS, de pérdida, destrucción y falsificación; no existen políticas de protección y privacidad de los datos personales de empleados, usuarios, proveedores y contratistas.

Así mismo, tampoco existe un procedimiento formal de revisión de la seguridad de la información, ni de cumplimiento y comprobación de las normas mínimas de seguridad de los activos.

4.2. Análisis de riesgos de los activos de información de KARISALUD IPS LTDA.

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad. Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones (ICONTEC).

De acuerdo con los resultados obtenidos a partir de la aplicación de los instrumentos de recolección de información en KARISALUD IPS LTDA., para evaluar la conformidad con el

estándar ISO/IEC 27002:2013, se hizo necesario, realizar un análisis de riesgos en cuanto a seguridad informática y de información, como complemento a la evaluación anterior, para determinar el nivel de riesgo al que se enfrenta la institución en mención y poder definir las recomendaciones necesarias para aceptarlo, reducirlo o transferirlo.

Para llevar a cabo este cometido, se utilizó una metodología estándar de análisis de riesgos, que consta de las siguientes fases:

- ***Identificación de Activos***. Implica determinar y clasificar los activos más relevantes para KARISALUD IPS.
- ***Identificación de Amenazas***: Se realiza una lista de las situaciones a las que están expuestos dichos activos.
- ***Valoración de activos***. Esta valoración se realiza especificando la magnitud del daño sobre el activo, en caso de materialización de la amenaza.
- ***Valoración de las amenazas***. Se valora la probabilidad de ocurrencia de la amenaza, teniendo en cuenta las siguientes consideraciones:

    - ¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos?
    - ¿Cuáles son nuestras vulnerabilidades?
    - ¿Cuántas veces ya han tratado de atacarnos?
    -

- ***Determinación del nivel de riesgo. Se obtiene del producto de la magnitud del daño por la probabilidad de ocurrencia de la amenaza.***

-

4.2.1. Identificación de Activos. Un activo o activos de información son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.).

El activo esencial de una organización es la información que maneja el sistema; y alrededor de ésta, se pueden identificar otros activos relevantes (Rec2):

- Los servicios que se pueden prestar gracias a la información disponible.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) que permiten alojar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

La aplicación de los distintos instrumentos de recolección permitió identificar los siguientes activos para KARISALUD IPS LTDA, clasificados como: Datos e Información, Sistemas e Infraestructura y Personal (Ver Cuadros 2, 3 y 4).

Cuadro 2. *Identificación de activos – Datos e Información.*

IDENTIFICACIÓN DE ACTIVOS			
DATOS E INFORMACIÓN			
No.	**ACTIVO/RECURSO**	**SI**	**NO**
1.	Documentos institucionales (Contratos, planes, políticas, manuales)	**X**	
2.	Directorio de contactos	**X**	
3.	Productos institucionales (investigaciones, proyectos)		**X**
4.	Correo electrónico	**X**	

Fuente: *Elaboración propia.*

Cuadro 2. *Continuación.*

5.	Bases de datos	**X**	
6.	Historias clínicas	**X**	
7.	Información de contraseñas	**X**	
8.	Respaldos de datos (Backup's)	**X**	
9.	Chat interno		**X**
10.	Información financiera	**X**	

Fuente: *Elaboración propia.*

Cuadro 3.
Identificación de activos – Sistemas e Infraestructura.

IDENTIFICACIÓN DE ACTIVOS			
SISTEMAS E INFRAESTRUCTURA			
No.	**ACTIVO/RECURSO**	**SI**	**NO**
1.	Equipos de la red cableada (router, módem, switch,…)		**X**
2.	Equipos de la red inalámbrica (router, punto de acceso,…)	**X**	
3.	Software de administración (contabilidad, citas, inventario,…)	**X**	
4.	Impresoras	**X**	
5.	Celulares		**X**
6.	Líneas telefónicas	**X**	
7.	Computadores (de escritorio, portátiles,…)	**X**	
8.	Dispositivos de almacenamiento (USB,…)	**X**	
9.	Equipos de laboratorio	**X**	
10.	Edificación (Recepción, Sala de espera, consultorios,…)	**X**	

Fuente: *Elaboración propia.*

Cuadro 4.
Identificación de activos - Personal

IDENTIFICACIÓN DE ACTIVOS
SISTEMAS E INFRAESTRUCTURA

No.	ACTIVO/RECURSO	SI	NO
1.	Junta Directiva	**X**	
2.	Gerencia	**X**	
3.	Auditoría	**X**	
4.	Atención al usuario	**X**	
5.	Personal técnico		**X**
6.	Personal informático interno		**X**
7.	Personal informático externo	**X**	
8.	Soporte técnico interno		**X**
9.	Soporte técnico externo	**X**	
10.	Personal de limpieza/interno	**X**	
11.	Servicio de mensajería/propio	**X**	
12.	Servicio de mensajería externo		**X**
13.	Vigilancia privada		**X**

Fuente: *Elaboración propia.*

4.2.2. Identificación de Amenazas. Se considera como amenaza, una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004)**.**

El origen de las amenazas puede ser diverso, desde:

- Desastres naturales, considerados como sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
- De origen industrial; sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
- Ataques intencionados; son fallos deliberados causados por las personas.

Para KARISALUD IPS LTDA., se realizó una lista de las amenazas más relevantes y a las que con más frecuencia está expuesta. Para la identificación de tales amenazas, se realizó la siguiente clasificación: actos originados por la criminalidad común, suceso de origen físico,

sucesos derivados de la negligencia de usuarios y decisiones institucionales (Ver Cuadros 5, 6 y 7).

Cuadro 5. *Identificación de amenazas – Actos originados por la criminalidad común.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

IDENTIFICACIÓN DE AMENAZAS

ACTOS ORIGINADOS POR LA CRIMINALIDAD COMÚN			
No.	**AMENAZA**	**SI**	**NO**
1.	Allanamiento (ilegal, legal)		**X**
2.	Persecución (civil, fiscal, penal)		**X**
3.	Orden de secuestro / Detención		**X**
4.	Sabotaje (ataque físico y electrónico)	**X**	
5.	Daños por vandalismo		**X**
6.	Extorsión		**X**
7.	Fraude / Estafa	**X**	
8.	Robo / Hurto (físico)	**X**	
9.	Robo / Hurto de información electrónica	**X**	
10.	Intrusión a Red interna	**X**	
11.	Infiltración	**X**	
12.	Virus / Ejecución no autorizado de programas	**X**	

Fuente: *Elaboración propia.*

Cuadro 6.
Identificación de amenazas – Sucesos derivados de la negligencia de usuarios.

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

IDENTIFICACIÓN DE AMENAZAS

SUCESOS DERIVADOS DE LA NEGLIGENCIA DE USUARIOS Y DECISIONES INSTITUCIONALES			
No.	**AMENAZA**	**SI**	**NO**
1.	Falta de inducción, capacitación y sensibilización sobre riesgos	**X**	
2.	Utilización de programas no autorizados / software pirateado		**X**
3.	Instalación de nuevos programas sin respaldo de datos		**X**
4.	Infección de sistemas a través de unidades portables sin escaneo	**X**	

Fuente*: Elaboración propia*.

Cuadro 6. *Continuación.*

5.	Manejo inadecuado de contraseñas	**X**	
6.	Compartir contraseñas o permisos a terceros no autorizados		**X**
7.	Falta de definición de perfil, privilegios y restricciones del personal	**X**	
8.	Falta de mantenimiento físico (proceso, repuestos e insumos)	**X**	
9.	Falta de actualización de software (proceso y recursos)	**X**	
10.	Fallas en permisos de usuarios (acceso a archivos)		**X**

11.	Acceso electrónico no autorizado a sistemas externos	**X**	
12.	Acceso electrónico no autorizado a sistemas internos	**X**	
13.	Red cableada expuesta para el acceso no autorizado		**X**
14.	Red inalámbrica expuesta al acceso no autorizado	**X**	
15.	Dependencia a servicio técnico externo	**X**	
16.	Falta de normas y reglas claras de seguridad	**X**	
17.	Falta de mecanismos de verificación de normas y reglas de seguridad	**X**	
18.	Ausencia de documentación	**X**	

Cuadro 7. *Identificación de amenazas – Sucesos de origen físico.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

IDENTIFICACIÓN DE AMENAZAS

SUCESOS DE ORIGEN FÍSICO			
No.	**AMENAZA**	**SI**	**NO**
1.	Incendio		**X**
2.	Inundación / deslave	**X**	
3.	Sismo		**X**
4.	Daños debido al polvo	**X**	
5.	Falta de ventilación	**X**	
6.	Electromagnetismo	**X**	
7.	Sobrecarga eléctrica	**X**	
8.	Falla de corriente (apagones)		**X**
9.	Falla de sistema /Daño disco duro	**X**	

Fuente: *Elaboración propia.*

4.2.3. Valoración de los Activos. Para realizar la valoración de los activos, se utiliza una escala que permite medir la magnitud del daño que sufre un elemento de información (activo), como consecuencia de un impacto causado por un ataque exitoso. En relación al impacto, es necesario considerar las siguientes opciones:

- Se pierde la información/conocimiento.
- Terceros podrían tener acceso a la información/conocimiento.
- La información ha sido manipulada o está incompleta.
- La información/conocimiento o persona no está disponible.

- Hay dudas acerca de la legitimidad de la fuente de la información.

Para valorar los elementos de información, se puede considerar la siguiente escala:

Cuadro 8. *Escala de valoración magnitud del daño sobre un activo de información.*

I: Insignificante	No causa ningún tipo de impacto o daño a la organización.
B: Bajo	Causa daño aislado, que no perjudica a ningún componente de la organización.
M: Medio	Provoca la desarticulación de un componente de la organización.
A: Alto	En el corto plazo desarticula a la organización.

Fuente: *Elaboración propia.*

Para KARISALUD IPS LTDA, se realizó la siguiente valoración de sus activos de información:

Cuadro 9. *Valoración de activos – Datos e Información.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA001

Empresa: **KARISALUD IPS LTDA** — Fecha Elaboración: 22/04/2014 — Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		

Fuente: *Elaboración propia.*

Cuadro 9: *Continuación*

DATOS E INFORMACIÓN							
1.	documentos institucionales (Contratos, planes, proyectos)				**X**		**J.C.G.G.**
2.	Directorio de contactos				**X**		
3.	Correo electrónico				**X**		
4.	Bases de datos				**X**		

5.	Historias clínicas				**X**		
6.	Información de contraseñas			**X**			
7.	Respaldos de datos (Backup)				**X**		
8.	Información financiera			**X**			
MARCAS UTILIZADAS							
IA001: Formato Identificación de Activos No. 1 **J.C.G.G.:** Jean Carlos García Guarín – Auditor Principal **Valoración magnitud del daño del activo:** **I = 1:** Insignificante - No causa ningún tipo de impacto o daño a la organización. **B = 2:** Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización. **M = 3:** Medio - Provoca la desarticulación de un componente de la organización. **A = 4:** Alto - En el corto plazo desarticula a la organización.							

Fuente: *Elaboración propia.*

Cuadro 10. *Valoración de activos – Sistemas e Infraestructura.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA002

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		
SISTEMAS E INFRAESTRUCTURA							
2.	Equipos de la red inalámbrica (router, punto de acceso,…)		**X**				**J.C.G.G.**
3.	Software de administración (contabilidad, citas,…)		**X**				
4.	Impresoras		**X**				
5.	Celulares	**X**					
6.	Líneas telefónicas	**X**					
7.	Computadores (de escritorio, portátiles,…)		**X**				
8.	Dispositivos de almacenamiento (USB,…)			**X**			

Fuente*: Elaboración propia*.

Cuadro 10. *Continuación.*

9.	Equipos de laboratorio				**X**		
10.	Edificación (Recepción, Sala de espera, consultorios,…)			**X**			
MARCAS UTILIZADAS							

IA002: Formato Identificación de Activos No. 2
J.C.G.G.: Jean Carlos García Guarín – Auditor Principal
Valoración magnitud del daño del activo:
I = 1: Insignificante - No causa ningún tipo de impacto o daño a la organización.
B = 2: Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización.
M = 3: Medio - Provoca la desarticulación de un componente de la organización.
A = 4: Alto - En el corto plazo desarticula a la organización.

Fuente: *Elaboración propia.*

Cuadro 11. *Valoración de activos – Personal.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA003

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		
PERSONAL							
1.	Junta Directiva				**X**		**J.C.G.G.**
2.	Gerencia				**X**		
3.	Auditoría				**X**		
4.	Atención al usuario			**X**			
5.	Personal técnico		**X**				**J.C.G.G.**
6.	Personal informático interno					No aplica	
7.	Personal informático externo			**X**			
8.	Soporte técnico interno					No aplica	
9.	Soporte técnico externo		**X**				
10.	Personal de limpieza/interno	**X**					
11.	Servicio de mensajería/propio	**X**					
12.	Servicio de mensajería externo					No aplica	
13.	Vigilancia privada					No aplica	
MARCAS UTILIZADAS							

IA003: Formato Identificación de Activos No. 3
J.C.G.G.: Jean Carlos García Guarín – Auditor Principal
Valoración magnitud del daño del activo:
I = 1: Insignificante - No causa ningún tipo de impacto o daño a la organización.
B = 2: Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización.
M = 3: Medio - Provoca la desarticulación de un componente de la organización.
A = 4: Alto - En el corto plazo desarticula a la organización.

Fuente: *Elaboración propia.*

4.2.4. Valoración de las Amenazas. Para darle un valor a cada una de las amenazas identificadas anteriormente, se utiliza una escala que permite medir la probabilidad de ocurrencia de la amenaza que podría causar perjuicio de disponibilidad, confidencialidad, integridad y autenticidad de la información o de los datos institucionales.

Para determinar la probabilidad de amenaza, se pueden tener en cuenta las siguientes consideraciones:

- ¿Cuál es el interés o la atracción por parte de individuos externos, de atacar la organización?
- ¿Cuáles son las vulnerabilidades más relevantes?
- ¿Cuántas veces han tratado de atacar la organización?

Para valorar la probabilidad de ocurrencia de cada amenaza, se puede utilizar la siguiente escala:

Cuadro 12. *Valoración probabilidad de ocurrencia de la amenaza.*

I: Insignificante	No existen condiciones que impliquen riesgo/ataque
B: Baja	Existen condiciones que hacen muy lejana la posibilidad del ataque
M: Mediana	Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo
A: Alta	La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

Fuente. *Elaboración propia*.

En KARISALUD IPS LTDA., se realizó la siguiente valoración de las amenazas identificadas como relevantes:

Cuadro 13. *Valoración probabilidad de amenaza – Actos originados por la criminalidad común.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT VA001

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Valorar la probabilidad de ocurrencia de las amenazas identificadas para KARISALUD IPS LTDA.

No.	ACTIVIDAD	PROB. OCURRENCIA				OBSERVACIONES	AUDITOR
		I	B	M	A		
ACTOS ORIGINADOS POR LA CRIMINALIDAD COMÚN							
1.	Allanamiento (ilegal, legal)	**X**					**J.C.G.G.**
2.	Persecución (civil, fiscal,…)	**X**					
3.	Orden de secuestro / detención	**X**					
4.	Sabotaje (ataque físico y electrónico)			**X**			
5.	Daños por vandalismo	**X**					

Fuente: *Elaboración propia.*

Cuadro 13. *Continuación*.

6.	Extorsión	**X**					
7.	Fraude / Estafa				**X**		
8.	Robo / Hurto (físico)			**X**			
9.	Robo / Hurto de información electrónica				**X**		
10.	Intrusión a Red interna				**X**		
11.	Infiltración				**X**		
12.	Virus / Ejecución no autorizado de programas			**X**			

MARCAS UTILIZADAS

VA001: Formato Valoración probabilidad de ocurrencia de la amenaza No. 1
J.C.G.G.: Jean Carlos García Guarín – Auditor Principal
Valoración probabilidad de ocurrencia de la amenaza:
I = 1: Insignificante - No existen condiciones que impliquen riesgo/ataque
B = 2: Bajo - Existen condiciones que hacen muy lejana la posibilidad del ataque
M = 3: Medio - Existen condiciones que hacen poco probable un ataque en el corto plazo
A = 4: Alto - La realización del ataque es inminente.

Fuente. *Elaboración propia*.

Cuadro 14. *Valoración probabilidad de amenaza – Sucesos derivados de la negligencia de usuarios.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT VA002

Empresa: **KARISALUD IPS LTDA** | Fecha Elaboración: 22/04/2014 | Fecha Revisión: 26/04/2014

Objetivo: Valorar la probabilidad de ocurrencia de las amenazas identificadas para KARISALUD IPS LTDA.

No.	ACTIVIDAD	PROB. OCURRENCIA				OBSERVACIONES	AUDITOR
		I	B	M	A		
SUCESOS DERIVADOS DE LA NEGLIGENCIA DE USUARIOS Y DECISIONES INSTITUCIONALES							
1.	Falta de inducción y capacitación sobre riesgos				**X**		**J.C.G.G.**
2.	Utilización de programas no autorizados		**X**				
3.	Instalación de programas sin respaldo de datos			**X**			
4.	Infección de sistemas a través de unidades portables				**X**		
5.	Manejo inadecuado de contraseñas			**X**			
6.	Compartir contraseñas o permisos a terceros		**X**				
7.	Falta de definición de perfil y restricciones del personal			**X**			
8.	Falta de mantenimiento físico (proceso, repuestos e insumos)			**X**			
9.	Falta de actualización de software (proceso y recursos)			**X**			
10.	Fallas en permisos de usuarios (acceso a archivos)		**X**				
11.	Acceso electrónico no autorizado a sistemas externos				**X**		
12.	Acceso electrónico no autorizado a sistemas internos				**X**		
13.	Red inalámbrica expuesta para el acceso no autorizado				**X**		
14.	Dependencia a servicio técnico externo				**X**		
15.	Falta de normas y reglas claras de seguridad				**X**		
16.	Falta de mecanismos de verificación de normas y reglas de seguridad				**X**		
17.	Ausencia de documentación				**X**		

MARCAS UTILIZADAS

VA002: Formato Valoración probabilidad de ocurrencia de la amenaza No. 2
J.C.G.G.: Jean Carlos García Guarín – Auditor Principal
Valoración probabilidad de ocurrencia de la amenaza:
I = 1: Insignificante - No existen condiciones que impliquen riesgo/ataque
B = 2: Bajo - Existen condiciones que hacen muy lejana la posibilidad del ataque
M = 3: Medio - Existen condiciones que hacen poco probable un ataque en el corto plazo
A = 4: Alto - La realización del ataque es inminente.

Fuente: *Elaboración propia.*

Cuadro 15. *Valoración probabilidad de amenaza – Sucesos de origen físico.*

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT VA003

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Valorar la probabilidad de ocurrencia de las amenazas identificadas para KARISALUD IPS LTDA.

No.	ACTIVIDAD	PROB. OCURRENCIA				OBSERVACIONES	AUDITOR
		I	B	M	A		
SUCESOS DE ORIGEN FÍSICO							
1.	Incendio	**X**					**J.C.G.G.**
2.	Inundación / deslave		**X**				
3.	Sismo	**X**					
4.	Daños debido al polvo			**X**			
5.	Falta de ventilación			**X**			
6.	Electromagnetismo		**X**				
7.	Sobrecarga eléctrica			**X**			
8.	Falla de corriente (apagones)		**X**				
9.	Falla de sistema- daño disco duro		**X**				

MARCAS UTILIZADAS

VA003: Formato Valoración probabilidad de ocurrencia de la amenaza No. 3
J.C.G.G.: Jean Carlos García Guarín – Auditor Principal
Valoración probabilidad de ocurrencia de la amenaza:
I = 1: Insignificante - No existen condiciones que impliquen riesgo/ataque
B = 2: Bajo - Existen condiciones que hacen muy lejana la posibilidad del ataque
M = 3: Medio - Existen condiciones que hacen poco probable un ataque en el corto plazo
A = 4: Alto - La realización del ataque es inminente.

Fuente: *Elaboración propia.*

4.2.5. Valoración del riesgo. Existen varios métodos de cómo valorar un riesgo. En el ámbito de la seguridad informática, se puede utilizar la siguiente fórmula matemática:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje X, representa la **probabilidad de amenaza** y el eje Y, la **magnitud de daño**. La

probabilidad de amenaza y magnitud del daño, pueden tomar condiciones entre **Insignificante** (1) y **Alta** (4).

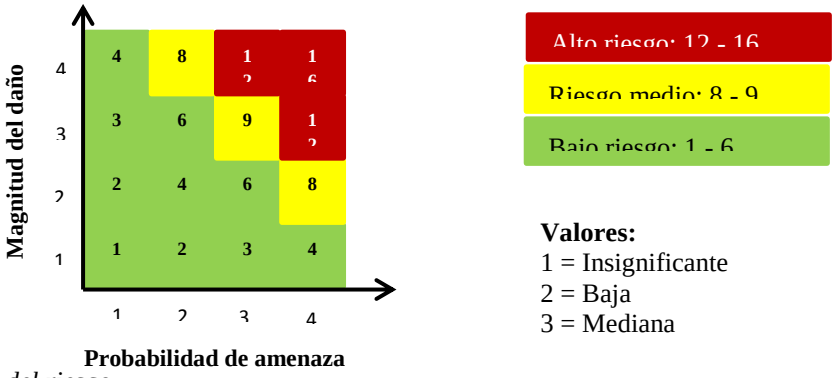

Figura 4. *Valoración del riesgo*.

Nota *Fuente: Elaboración propia*.

De acuerdo con la información obtenida a partir de entrevistas, listas de chequeo, formatos de observación, entre otros, se llevó a cabo el proceso de análisis de riesgos, con las actividades descritas en los apartados anteriores. El consolidado del proceso, se muestra en la siguiente matriz, (Ver Cuadros 16, 17 y 18) que permitirá visualizar el nivel de riesgo de KARISALUD IPS LTDA., en lo que respecta a la seguridad informática y de la información.

Cuadro 16. *Matriz de riesgos – Datos e Información*

DATOS E INFORMACIÓN	VALORACIÓN MAGNITUD DEL DAÑO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA																																				
		ACTOS ORIG. CRIMINALIDAD COMÚN													SUCESOS DERIVADOS DE LA NEGLIGENCIA DE USUARIOS																			SUCESOS DE ORIGEN FÍSICO								
		Allanamiento (legal, ilegal)	Persecución civil, fiscal, penal	Orden de secuestro / detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Falta de inducción y capacitación sobre riesgos	Utilización de programas no autorizados	Instalación de programas sin respaldo de datos	Infección de sist. a través de unidades portables	Manejo inadecuado de contraseñas	Compartir contraseñas o permisos a terceros	Falta de definición de perfiles y rest. del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sist. externos	Acceso electrónico no autorizado a sist. internos	Red inalámbrica expuesta para el acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras de seguridad	Falta de mecanismos de verif. de normas de seguridad	Ausencia de documentación	Incendio	inundación / deslave	Sismos	Daños debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Fallas de sistema - daños en el disco duro
		1	1	1	3	1	1	4	3	4	4	4	3	4	2	3	4	3	2	3	3	3	2	4	4	4	4	4	4	4	1	2	1	3	3	2	3	2	2
Documentos institucionales	4																																						
Directorio de contactos	4																																						
Correo electrónico	4																																						
Bases de datos	4																																						
Historias clínicas	4																																						
Información de contraseñas	3																																						
Respaldos de datos (Backup's)	4																																						
Información financiera	3																																						

Fuente: *Elaboración propia.*

Cuadro 17. *Matriz de riesgos – Sistemas e infraestructura.*

SISTEMAS E INFRAESTR.	VALORACIÓN MAGNITUD DEL DAÑO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA																																				
		ACTOS ORIG. CRIMINALIDAD COMÚN												SUCESOS DERIVADOS DE LA NEGLIGENCIA DE USUARIOS																SUCESOS DE ORIGEN FÍSICO								
		Allanamiento (legal, ilegal)	Persecución civil, fiscal, penal	Orden de secuestro / detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Falta de inducción y capacitación sobre riesgos	Utilización de programas no autorizados	Instalación de programas sin respaldo de datos	Infección de sist. a través de unidades portables	Manejo inadecuado de contraseñas	Compartir contraseñas o permisos a terceros	Falta de definición de perfiles y rest. del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sist. externos	Acceso electrónico no autorizado a sist. internos	Red inalámbrica expuesta para el acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras de seguridad	Falta de mecanismos de verif. de normas de seguridad	Ausencia de documentación	Incendio	inundación / deslave	Sismos	Daños debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Fallas de sistema - daños en el disco duro
		1	1	1	3	1	1	4	3	4	4	4	3	4	2	3	4	3	2	3	3	3	2	4	4	4	4	4	4	4	1	2	1	3	3	2	3	2	2
Equipos red inalámbrica	2																																						
Software de administración	2																																						
Impresoras	2																																						
Celulares	1																																						
Líneas telefónicas	1																																						
Computadores	2																																						
Dispositivos almacenamiento	3																																						
Equipos de laboratorio	4																																						
Edificación - locaciones	3																																						

Fuente: *Elaboración propia.*

Cuadro 18. *Matriz de riesgos – Personal.*

PERSONAL	VALORACIÓN MAGNITUD DEL DAÑO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA																																			
		ACTOS ORIG. CRIMINALIDAD COMÚN												SUCESOS DERIVADOS DE LA NEGLIGENCIA DE USUARIOS																SUCESOS DE ORIGEN FÍSICO								
		Allanamiento (legal, ilegal)	Persecución civil, fiscal, penal	Orden de secuestro / detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Falta de inducción y capacitación sobre riesgos	Utilización de programas no autorizados	Instalación de programas sin respaldo de datos	Infección de sist. a través de unidades portables	Manejo inadecuado de contraseñas	Compartir contraseñas o permisos a terceros	Falta de definición de perfiles y rest. del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sist. externos	Acceso electrónico no autorizado a sist. internos	Red inalámbrica expuesta para el acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras de seguridad	Falta de mecanismos de verif. de normas de seguridad	Ausencia de documentación	Incendio	inundación / deslave	Sismos	Daños debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Fallas de sistema - daños en el disco duro
		1	1	1	3	1	1	4	3	4	4	4	3	4	2	3	4	3	2	3	3	3	2	4	4	4	4	4	4	4	1	2	1	3	3	2	3	2	2
Junta Directiva	4																																						
Gerencia	4																																						
Auditoría	4																																						
Atención al usuario	3																																						
Personal técnico	2																																						
Personal informático externo	3																																						
Soporte técnico externo	2																																						
Personal de limpieza interno	1																																						
Servicio de mensajería propio	1																																						

Fuente: *Elaboración propia.*

La anterior matriz (clasificada en cada uno de los elementos de información), permite evidenciar lo siguiente:

En la primera clasificación, **DATOS E INFORMACIÓN,** resulta demasiado evidente el alto riesgo al que se encuentran expuestos dichos activos, debido a las vulnerabilidades existentes en la empresa (información obtenida de la aplicación de los instrumentos de recolección) y a la alta probabilidad de ocurrencia de las amenazas que pueden generar un impacto negativo para la prestación de los servicios que ofrece KARISALUD IPS LTDA.

La gran debilidad se centra en la ausencia de procedimientos formales para proteger la información; así como de normas y políticas institucionales que estén orientadas a la seguridad no solo de los activos institucionales, sino también de los datos personales tanto de empleados y directivos como de usuarios finales.

Esta carencia de controles, pone en alto riesgo la confidencialidad, disponibilidad e integridad de la información que la IPS utiliza y produce para el óptimo desarrollo de sus actividades, el cumplimiento de sus metas organizacionales y la consecuente satisfacción de sus usuarios.

En lo que respecta a la segunda clasificación **SISTEMAS E INFRAESTRUCTURA,** aunque hay muy pocas secciones marcadas como de alto riesgo, cabe resaltar que se requieren

controles en lo relacionado con la seguridad física y ambiental, para poder reducir el impacto de un ataque a la infraestructura de hardware y software de la institución.

Se requieren procedimientos documentados para la correcta administración del hardware, del software y de las instalaciones; así como de la protección física de las copias de respaldo.

Finalmente, en la tercera clasificación, **PERSONAL**, existe una gran dependencia del nivel directivo de la empresa, así como del personal informático y de soporte técnico. La gran mayoría de las funciones de administración de seguridad de la información no se encuentran segregadas, lo que aumenta el riesgo de pérdida parcial o total de la información, así como de la imagen corporativa.

4.2.6 Guía de Aplicabilidad de controles de seguridad de la información de acuerdo con el estándar ISO/IEC 27002:2013. La presente Guía contempla los criterios de aplicabilidad contenidos en el estándar ISO 27002:2013, en lo relacionado con la gestión de la seguridad de la información.

Es indispensable que el nivel directivo de KARISALUD IPS LTDA., se comprometa con el cumplimiento, sostenibilidad y aplicabilidad del Sistema de Gestión de Seguridad de la Información SGSI, junto con sus políticas y procedimientos definidos y documentados, con el fin de proteger los recursos de información de la Institución; así mismo, realizar una permanente

gestión de los riesgos a los que se enfrenta, de tal manera que se pueda reducir el impacto de la materialización de las amenazas identificadas y superar las vulnerabilidades presentes.

A continuación se presenta la Guía de Aplicabilidad del Sistema de Gestión de Seguridad de la Información para KARISALUD IPS LTDA. (Ver Cuadro 20), teniendo en cuenta el estándar ISO/IEC 27002:2013.

La guía en mención, está compuesta de:

- Objetivo de control
- Controles
- Criterio de aplicabilidad (SI - NO)
- Justificación

Cuadro 19. *Guía de aplicabilidad SGSI ISO 27002:2013*

GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

OBJETIVO DE CONTROL	CONTROLES	JUSTIFICACIÓN
A5. POLÍTICAS DE SEGURIDAD		
5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN	5.1.1 Conjunto de políticas para la seguridad de la información	Es necesario establecer una política de seguridad de la información para informar y concientizar a todos los empleados, directivos y partes interesadas (contratistas y proveedores) sobre los riesgos a los que están expuestos, así como los controles implementados para evitar la materialización de estos riesgos. La revisión de las políticas de seguridad de la información debería tener en cuenta los resultados de las revisiones por parte del nivel directivo de KARISALUD IPS LTDA. De igual forma, se sugiere diseñar, implementar, socializar a los diferentes niveles de la Institución, los lineamientos contemplados en el documento de Políticas de Seguridad de la Información, para que se adopte una cultura de la protección de la información y de los demás activos de información de la institución.
	5.1.2 Revisión de las políticas para la seguridad de la información.	
A6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1 ORGANIZACIÓN INTERNA	6.1.1 Asignación de responsabilidades para la segur. de la información	La organización mediante su política de seguridad de la información debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma velar por mantener protegido su información mediante la revisión del sistema de gestión de seguridad de la información. Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y
	6.1.2 Segregación de tareas	
	6.1.3 Contacto con las autoridades	
	6.1.4 Contacto con grupos de interés especial	

Fuente: *Elaboración propia.*

Cuadro 20. *Continuación.*

	6.1.5 Seguridad de la información en la gestión de proyectos.	documentando claramente los niveles de autorización.
A7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
7.1 ANTES DE LA CONTRATACIÓN	7.1.1 Investigación de antecedentes	Se recomienda establecer un acuerdo de confidencialidad para cada uno de los empleados de KARISALUD IPS en el momento de su contratación o cuando haya algún cambio de puesto de trabajo, que contemple los requerimientos para proteger la información, utilizando términos legalmente ejecutables y especificando entre otros aspectos, el tipo de información que debe protegerse, la duración esperada del acuerdo, las responsabilidades para usar información confidencial, así como para evitar su divulgación, condiciones específicas de terminación del contrato laboral y las sanciones impuestas para los casos de incumplimiento de dicho acuerdo El personal de la organización en el desarrollo de las actividades para las cuales fueron contratados, interactúa permanentemente con la información; en tal sentido es necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes con respecto a seguridad de la información. De igual forma, es necesario capacitar al personal permanentemente en temas de seguridad de la información según sea pertinente para sus funciones laborales.
	7.1.2 Términos y condiciones de contratación	
7.2 DURANTE LA CONTRATACIÓN	7.2.1 Responsabilidades de gestión.	
	7.2.2 Concienciación, educación y capacitación en seguridad. de la información	
	7.2.3 Proceso disciplinario	
7.3 CESE O CAMBIO DE PUESTO DE TRABAJO	7.3.1 Cese o cambio de puesto de trabajo	
A8. GESTIÓN DE ACTIVOS		
8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	8.1.1 Inventario de activos.	La IPS dentro del proceso de implementación y mantenimiento del sistema de gestión de seguridad de la información debe realizar un inventario de todos sus activos de información, e identificar y documentar los propietarios de estos, realizar un inventario de los más importantes, y también garantizar el uso adecuado de los mismos a través de reglas documentadas e implementadas. De igual manera, se recomienda establecer una clasificación específica para KARISALUD IPS LTDA., que indique los niveles de protección de acuerdo con la importancia de los mismos y el valor comercial que representan para la Institución, así como documentar e implementar reglas para el uso aceptable y seguro de los activos de información.
	8.1.2 Propiedad de los activos.	
	8.1.3 Uso aceptable de los activos.	
	8.1.4 Devolución de activos.	
8.2 CLASIFICACIÓN DE LA INFORMAC.	8.2.1 Directrices de clasificación	
	8.2.2 Etiquetado y manipulado de la información	
	8.2.3 Manipulación de activos	
8.3	8.3.1 Gestión de soportes extraíbles.	

MANEJO DE LOS SOPORTES DE ALMACENAMIENTO	8.3.2 Eliminación de soportes	
	8.3.3 Soportes físicos en tránsito.	
A9. CONTROL DE ACCESOS		
9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS	9.1.1 Política de control de accesos.	KARISALUD IPS presta servicios asistenciales de salud para lo cual es importante establecer controles que permitan asegurar que los propietarios de activos de información controlan el acceso a la información que utilizan para sus operaciones La IPS para su operación cuenta con una red LAN inalámbrica que soporta las actividades de los diferentes usuarios, por lo tanto es necesario establecer controles para asegurar que los usuarios solo tienen acceso a los servicios para los cuales están autorizados.
	9.1.2 Control de acceso a las redes y servicios asociados.	
9.2 GESTIÓN DE ACCESO DE USUARIO	9.2.1 Gestión de altas/bajas en el registro de usuarios	Se hace necesario establecer un procedimiento formal para la gestión de los derechos de acceso de los usuarios de los sistemas de información, donde se entregue un documento a cada usuario indicando la información relacionada con el acceso (usuario y contraseña) y los requerimientos de protección de la información que tendrá bajo su responsabilidad.
	9.2.2 Gestión de los derechos de acceso asignados a usuarios	
	9.2.3 Gestión de los derechos de acceso con privilegios especiales	
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	
	9.2.5 Revisión de los derechos de acceso de los usuarios	
	9.2.6 Retirada o adaptación de los derechos de acceso	
9.3 RESPONSABILIDADES DEL USUARIO	9.3.1 Uso de información confidencial para la autenticación.	
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	9.4.1 Restricción del acceso a la información	
	9.4.2 Procedimientos seguros de inicio de sesión.	
	9.4.3 Gestión de contraseñas de usuario.	
	9.4.4 Uso de herramientas de administración de sistemas.	

	9.4.5 Control de acceso al código fuente de los programas.	
A10. CIFRADO		
10.1 CONTROLES CRIPTOGRÁFICOS	10.1.1 Política de uso de los controles criptográficos.	KARISAUD IPS debe establecer controles criptográficos para los sistemas de información que se manejan en los diferentes niveles de la Institución, con el objetivo de garantizar la confidencialidad e integridad de la información. Establecer protocolos y documentar los procedimientos para la gestión de los derechos y niveles de acceso a los sistemas de información.
	10.1.2 Gestión de claves.	
A11. SEGURIDAD FÍSICA Y AMBIENTAL		
11.1 ÁREAS SEGURAS	11.1.1 Perímetro de seguridad física.	KARISALUD IPS, debe diseñar e implementar un Plan de Contingencias y un documento de Políticas de Seguridad, que contemple los riesgos de seguridad física. Para esto, se sugiere: Implantar sistemas biométricos que permitan controlar de forma más eficiente el acceso a las áreas críticas de IPS. Instalar alarmas contra incendios, detectores de humo y salidas de emergencia, para minimizar el impacto que puede provocar la presencia de una catástrofe ambiental. Construir o adecuar un espacio fuera de las instalaciones de la IPS, con las medidas de seguridad física necesarias para almacenar las copias de respaldo. Realizar campañas de sensibilización sobre la protección tanto de los equipos como de la información que cada funcionario, específicamente los que manejan sistemas de información, tiene bajo su responsabilidad.
	11.1.2 Controles físicos de entrada	
	11.1.3 Seguridad de oficinas, despachos y recursos	
	11.1.4 Protección contra las amenazas externas y ambientales.	
	11.1.5 El trabajo en áreas seguras.	
	11.1.6 Áreas de acceso público, carga y descarga.	La infraestructura física de la IPS no cuenta con áreas de carga o despacho. El edificio solo tiene una entrada principal con su respectiva recepción; por tal razón no es necesario establecer controles de seguridad para proteger las áreas de despacho o carga.
	11.2.1 Emplazamiento y protección de equipos	Para el desarrollo de las actividades de KARISALUD IPS se utiliza equipos tales como servidores, computadores de escritorio, portátiles, impresoras, entre otros, en donde se procesa la información de los diferentes servicios que ofrece la Institución; por tal razón es necesario establecer controles que permitan reducir la ocurrencia de eventos que puedan generar la pérdida parcial o total de los datos, daño, robo o
	11.2.2 Instalaciones de suministro	
	11.2.3 Seguridad del cableado.	
	11.2.4 Mantenimiento de los equipos.	

11.2 SEGURIDAD DE LOS EQUIPOS	11.2.5 Salida de activos fuera de las dependencias de la empresa	interrupción de los servicios asistenciales y administrativos de la IPS. Así mismo, se recomienda establecer protocolos documentados para el retiro de los equipos fuera de las instalaciones, y para la reutilización o retirada segura de los mismos.
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	
	11.2.8 Equipo informático de usuario desatendido.	
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	
A12. SEGURIDAD EN LA OPERATIVA		
12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN	12.1.1 Documentación de procedimientos de operación	Este objetivo de control no aplica para KARISALUD IPS LTDA, ya que no tiene dentro de su objeto social, la producción y mantenimiento de software y/o aplicaciones.
	12.1.2 Gestión de cambios.	
	12.1.3 Gestión de capacidades	
	12.1.4 Separación de entornos de desarrollo, prueba y producción	
12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO	12.2.1 Controles contra el código malicioso	Para el desarrollo de las actividades de la IPS se utilizan distintos servicios que pueden afectar el correcto funcionamiento de los activos de información como equipos, aplicaciones, entre otros; por lo tanto es importante establecer controles de seguridad que permitan la prevención, detección y corrección de la acción de códigos maliciosos así como también procedimientos de sensibilización a usuarios.
12.3 COPIAS DE SEGURIDAD.	12.3.1 Copias de seguridad de la información	En cuanto a las copias de seguridad, se debe diseñar e implementar una política de respaldo que contenga los procedimientos para la realización de Backup y su debida restauración; así mismo, que contemple las acciones para definir el nivel necesario de respaldo de la información y la extensión y frecuencia de dicho procedimiento, de acuerdo con los requerimientos propios de la Institución.
12.4 REGISTRO DE ACTIVIDAD Y	12.4.1 Registro y gestión de eventos de actividad	Se recomienda establecer controles de seguridad definidos, documentados, implementados, socializados y evaluados, que permitan la detección oportuna de actividades de procesamiento de información no autorizada y herramientas
	12.4.2 Protección de los registros de información	

SUPERVISIÓN.	12.4.3 Registros de actividad del administrador y operador del sistema	para investigaciones futuras de incidentes de seguridad de la información.
	12.4.4 Sincronización de relojes.	
12.5 CONTROL DEL SW EN EXPLOTACIÓN	12.5.1 Instalación del software en sistemas en producción.	Es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los usuarios, se restringe la posibilidad de instalación de programas y/o aplicativos
12.6 GESTIÓN DE LA VULNERAB. TÉCNICA	12.6.1 Gestión de las vulnerabilidades técnicas	KARISALUD IPS tiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto es necesario establecer controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas.
	12.6.2 Restricciones en la instalación de software	
12.7 CONSIDERACIONES DE LAS AUDITORÍAS DE LOS SIST. DE INF.	12.7.1 Controles de auditoría de los sistemas de información.	Es necesario mantener un registro de auditoría de todos los procedimientos realizados en las distintas aplicaciones instaladas.
A13. SEGURIDAD EN LAS TELECOMUNICACIONES		
13.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES	13.1.1 Controles de red.	Se recomienda implementar controles para garantizar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no autorizados.
	13.1.2 Mecanismos de seguridad asociados a servicios en red	
	13.1.3 Segregación de redes.	
13.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS	13.2.1 Políticas y procedimientos de intercambio de información.	Se debieran establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información con otras instituciones mediante el uso de todos los tipos de medios de comunicación. Se recomienda implementar controles para garantizar la protección de la información que transita a través de la red de datos; estos controles incluyen, segregación de responsabilidades, asignación de privilegios a los usuarios de las redes, procedimientos documentados para mantener la disponibilidad de los servicios de la red, entre otros.
	13.2.2 Acuerdos de intercambio.	
	13.2.3 Mensajería electrónica.	
	13.2.4 Acuerdos de confidencialidad y secreto	
A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		

14.1 REQUISITOS DE SEGURIDAD DE LOS SIST. DE INFORM.	14.1.1 Análisis y especificación de los requisitos de seguridad.	Se recomienda que para los contratos de adquisición de software, se consideren los siguientes puntos: Contratos de licencias, propiedad de códigos, derechos de propiedad intelectual; certificación de la calidad y exactitud del trabajo llevado a cabo; contratos de depósito en custodia en el evento de la falla de una tercera persona; requerimientos contractuales para la funcionalidad de calidad y seguridad del código; prueba antes de la instalación para detectar códigos maliciosos y troyanos.
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	
	14.1.3 Protección de las transacciones por redes telemáticas	
14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.	14.2.1 Política de desarrollo seguro de software	Este objetivo de control no aplica para KARISALUD IPS LTDA, puesto que internamente no se llevan procesos de desarrollo y soporte de software.
	14.2.2 Procedimientos de control de cambios en los sistemas.	
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	
	14.2.4 Restricciones a los cambios en los paquetes de software.	
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	
	14.2.6 Seguridad en entornos de desarrollo.	
	14.2.7 Externalización del desarrollo de software	
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	
	14.2.9 Pruebas de aceptación.	
14.3 DATOS DE PRUEBA	14.3.1 Protección de los datos utilizados en pruebas.	Este objetivo de control no aplica para KARISALUD IPS LTDA, puesto que internamente no se llevan procesos de desarrollo de software.
A15. RELACIONES CON SUMINISTRADORES		
15.1 SEGURIDAD DE LA INFORMACIÓN EN	15.1.1 Política de seguridad de la información para suministradores	Establecer formalmente protocolos para la prestación de servicios ofrecidos por terceros, que contemple entre otras cosas, el tratamiento del riesgo al proporcionar información confidencial, controles para garantizar el
	15.1.2 Tratamiento del riesgo	

LAS RELACIONES CON SUMINIST.	dentro de acuerdos de suministradores.	cumplimiento de los acuerdos y procedimientos para la gestión del cambio en dichos servicios.
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	
15.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	
	15.2.2 Gestión de cambios en los servicios prestados por terceros	
A16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	16.1.1 Responsabilidades y procedimientos.	Se recomienda establecer un procedimiento formal para el reporte de eventos de seguridad, así como el establecimiento de canales seguros para el reporte de los mismos. Junto con éste, procedimientos para dar respuesta oportuna a dichos incidentes, asignando responsables o un punto de contacto, que atienda tales solicitudes. Por otra parte, se sugiere entrenar a los usuarios de los sistemas de información y de aquellos que tengan activos de información a su cargo, sobre las diversas actividades de identificación y reporte de eventos de seguridad.
	16.1.2 Notificación de los eventos de seguridad de la información.	
	16.1.3 Notificación de puntos débiles de la seguridad.	
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	
	16.1.5 Respuesta a los incidentes de seguridad	
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	
	16.1.7 Recopilación de evidencias.	
A17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
17.1 CONTINUIDAD DE LA SEGURIDAD DE LA	17.1.1 Planificación de la continuidad de la seguridad de la información.	Se recomienda implementar un proceso de gestión de la continuidad del negocio, PCN, bajo estándares internacionales reconocidos y probados, para minimizar el impacto en caso de pérdida parcial o total de sus funciones de
	17.1.2 Implantación de la	

INFORMACIÓN	continuidad de la seguridad de la información.	operación, provocada por eventos no intencionados como desastres naturales, accidentes, fallas en los equipos o cualquier otro incidente cometido de forma deliberada. El proceso de gestión del PCN debe incluir la intervención del nivel directivo de KARISALUD IPS y de cada una de las áreas del nivel operativo, de tal manera que se puedan tomar decisiones para proveer soluciones al respecto. Dicho proceso requiere entre otras cosas, la realización permanente de análisis y evaluación de riesgos, que permitan identificar amenazas y vulnerabilidades en los elementos de información y calcular el impacto que la materialización de las mismas pueda generar en el desarrollo de las operaciones de la IPS.
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
17.2 REDUNDANCIAS	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
A18. CUMPLIMIENTO		
18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	18.1.1 Identificación de la legislación aplicable	Se sugiere definir, documentar y actualizar todos los requerimientos legales, reguladores y contractuales y el enfoque de la IPS para satisfacer esos requerimientos, para cada sistema de información. De igual forma se recomienda, que para efecto de revisión y publicación de procedimientos relacionados con sistemas de información, arquitecturas de hardware y software, telecomunicaciones, se cuente con la asesoría de un experto, para que el resultado de dicha evaluación pueda ser lo más objetivo posible.
	18.1.2 Derechos de propiedad intelectual (DPI)	
	18.1.3 Protección de los registros de la organización	
	18.1.4 Protección de datos y privacidad de la información personal.	
	18.1.5 Regulación de los controles criptográficos.	
18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	18.2.1 Revisión independiente de la seguridad de la información.	
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	
	18.2.3 Comprobación del cumplimiento.	

Conclusiones

La investigación realizada en torno al diseño de una guía de aplicabilidad de controles de seguridad para la IPS KARISALUD LTDA de acuerdo con el Estándar ISO/IEC 27002:2013, permitió constatar que:

- Se elaboró el diagnóstico que permitió evidenciar el estado actual de KARISALUD IPS LTDA., en lo relacionado con la gestión de la seguridad de la información, para lo cual se hizo necesario realizar una auditoría de cumplimiento bajo el estándar ISO/IEC 27002:2013.

- Se realizó un análisis de riesgos, identificando los activos de información y las amenazas a las cuales se encuentran expuestos dichos activos. Así mismo, se determinó el nivel de riesgo de los mismos y se realizaron recomendaciones al respecto.

- Finalmente, se diseñó un documento que contiene los criterios de aplicabilidad del estándar ISO/IEC 27002:2013, de acuerdo con todos sus dominios, objetivos de control y controles.

Además, los datos obtenidos en la investigación sobre la gestión de los recursos tecnológicos de la Universidad Francisco de Paula Santander Ocaña, permitieron dimensionar el

estado actual de dicha gestión y estructurar a partir del mismo, una alternativa para mediar en la búsqueda de soluciones para dicha situación.

La situación relacionada con la gestión de los recursos tecnológicos de la Universidad Francisco de Paula Santander Ocaña, no se ve a nivel institucional como un hecho aislado, sino como un problema que requiere atención prioritaria, pues afecta los índices de calidad institucionales.

El Plan Estratégico de Tecnologías de la Información propuesto, se estructuró de forma tal que todas las iniciativas de TI, puedan soportar las actividades académicas y administrativas de la Universidad y se alineen a ellas para el logro de su misión institucional.

Recomendaciones

Para garantizar un adecuado Sistema de Gestión de la Seguridad de la Información, es necesario que el nivel directivo de la organización se comprometa con el diseño, la implementación y permanente evaluación de las políticas y procedimientos necesarias para garantizar que la información que utiliza y/o genera, se encuentra debidamente respaldada y de esta manera, contribuya con el logro de las metas institucionales, la satisfacción del cliente y la confianza de los inversionistas.

KARISALUD IPS LTDA., debe propiciar un ambiente de seguridad para cada uno de los activos organizacionales, desde los recursos físicos (hardware, instalaciones), intangibles (software, datos, información) hasta el recurso humano, elementos imprescindibles para el éxito institucional.

De acuerdo con los resultados obtenidos, producto del diagnóstico realizado a KARISALUD IPS LTDA., en términos de seguridad informática y de información, se propone lo siguiente:

- Diseñar e implementar un documento de políticas de seguridad de la información, que tenga en cuenta las necesidades de la IPS. Así mismo, establecer criterios y procedimientos formales para la revisión, que pudieran sugerir modificaciones al documento.

- Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y documentando claramente los niveles de autorización.

- Garantizar que los empleados, contratistas y terceros comprendan el nivel de responsabilidad sobre la información, y posean las competencias personales y laborales para cada puesto de trabajo.

- Establecer formalmente protocolos para la prestación de servicios ofrecidos por terceros (proveedores, contratistas,…), que tenga en cuenta, el tratamiento del riesgo al momento de intercambiar información confidencial y los mecanismos de control necesarios para garantizar el cumplimiento de los acuerdos establecidos.

Referencias

(s.f.). Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/elementos_informacion/

(s.f.). Obtenido de Recuperado de : https://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf

(ICONTEC), I. C. (2006). Norma Tecnica NTC-ISO IEC COLOMBIANA 27001 . Recuperado el 12 de 05 de 2016, de Recuperado de http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Avendaño, W. A. (2015). . Diseño de un modelo de análisis y diagnóstico del nivel de madurez en sí para en Mipymes de asesoría legal y oficinas de abogados, como base para la implementación de la norma iso27002. . Obtenido de Recuperado de http://repository.poligran.edu.co/bitstream/10823/744/1/Avenda%C3%B1o%20Arenales%20-%20ESI%20trabajo%20de%20Grado.pdf

Erb, M. (2015). Gestion de riesgo en la seguridad Informatica. Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

(s.f.). Gerente en conversaciones previas a la viabilidad .

ICONTEC. (s.f.). ISO/IEC 17799:2005. Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

Informacion, C. E. (2010). Sistema de gestion de seguridad de la seguridad de la iunformacion, ISO 27001. Obtenido de Recuperado de http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

Instituto Departamental de Salud. (2016). https://ids.gov.co/web/.

Markus, E. (2015). Gestion de riesgo en la seguridad informatica. Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/elementos_informacion/

Markus, E. (2015). Gestión de riesgo en la seguridad informática. Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Mendoza, M. A. (2015). ¿ Que es la declaracion de Aplicabilidad (SoA) y para que sirve? Obtenido de Recuperado de http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

Ministerio de Proteccion Social. (2006). Decreto 1011 . Bogota.

nstituto Nacional de Transparencia, a. a. (2015). Guìa para implementar un Sistema de Gestión de Seguridad de Datos Personales. Obtenido de Recuperado de http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf

Pacheco, M. S. (2013). Elaboración de políticas de seguridad física y ambiental basados en el estándar internacional ISO/IEC 27002:. Obtenido de Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/901/1/27980.pdf

Reyes, M. A. (2015). Diseño de un plan estratégico de tecnologías de información para la Universidad Francisco de Paula Santander Ocaña. . Obtenido de Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/814/1/27740.pdf

Rojas, H. V. (2014). Plan de Implementacion de la ISO/TEC 27001/2013. Recuperado el 12 de 05 de 2016, de Recuperado de de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40297/1/hrojasvTFM1214.pdf

Ruiz, J. J. (2014). Analisis de Riesgo de la Seguridad de la Informacion para la Institucion Universitaria . Obtenido de Recuperado de http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf

Santamaria, j. R. (2014). Manual de seguridad de la informacion para un organismo del estado colombiano. Obtenido de Recuperado de : http://repository.unimilitar.edu.co/bitstream/10654/11730/1/JULIANA%20ANDREA%20SANTAMARIA%20RAMIREZ1.pdf

www.protejete.wordpress.com. (s.f.). Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

www.protejete.wordpress.com. (2015). Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/definicion_si/

www.protejete.wordpress.com. (2015). Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

www.protejete.wordpress.com. (2015). Obtenido de Recuperado de https://protejete.wordpress.com/gdr_principal/retos_seguridad/

Apéndices

Apéndice 1. Autorización uso de instrumentos de indagación.

Las abajo firmantes, María Alejandra Arrieta Sánchez, Magreth Rossio Sanguino Reyes y Cindy Lorena Lobo Sánchez, autoras del proyecto de grado titulado "Diseño de un Plan Estratégico de Tecnologías de Información para la Universidad Francisco de Paula Santander Ocaña", autorizamos a los estudiantes de la Especialización en Informática Educativa Jean Carlos y Orozco, para que hagan uso de los instrumentos de indagación referenciados en los Apéndices A y B, en su proyecto de grado titulado "Diseño de una Guía de Aplicabilidad de Controles de Seguridad para la IPS KARISALUD Ltda., de Acuerdo con el Estándar ISO/IEC 27002:2013"

Se firma el original, a los 22 días del mes de abril de 2016.

María Alejandra Arrieta Sánchez **Magreth Rossio Sanguino Reyes**

Cindy Lorena Lobo Sánchez

Apéndice 2. Entrevista No. 1.

Kari Salud I.P.S. LTDA	Universidad Francisco de Paula Santander Ocaña - Colombia
DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013	
R/PT No. EN001	
Empresa:	**KARISALUD IPS LTDA.**
Entrevistado:	**Gerente**
Objetivo: Evaluar el grado de cumplimiento de las actividades relacionadas con la seguridad de la información, de acuerdo con lo establecido en el estándar ISO 27002:2013	
ÍTEM	**PREGUNTA**
1.	¿Existe formalmente una política de seguridad que establezca los parámetros para la protección de los activos informáticos y de información?
RTA	
2.	¿Cómo se ha dado el proceso de socialización de estas políticas a cada uno de los miembros de la Institución?
RTA	
3.	¿Existen responsables de la protección de los activos de información con sus funciones claramente definidas?
RTA	
4.	¿Las responsabilidades en cuanto a la seguridad de los activos de información, se encuentran segregadas para reducir la posibilidad de fraude o pérdida de dichos activos?
RTA	
5.	¿KARISALUD IPS cuenta con procedimientos definidos y documentados que establezcan el protocolo a seguir en el momento en el que se presente un incidente de seguridad que pueda poner en riesgo el normal funcionamiento de la Institución?
RTA	
6.	¿Existen procedimientos documentados para la realización de copias de respaldo, capacitación, mantenimiento de hardware y software, adquisición de tecnología, reporte de incidentes, entre otros?
RTA	
7.	Cuando se establecen acuerdos con terceros, ¿existe una persona o equipo responsable de la verificación del cumplimiento de los servicios ofrecidos por ellos?
RTA	
8.	¿Se realiza algún tipo de seguimiento y/o revisión de los servicios y/o productos

	suministrados por terceros, en lo relacionado con las condiciones de protección y confidencialidad de la información que se utiliza para tal efecto?
RTA	
9.	¿Qué controles existen para la detección, prevención y recuperación contra código malicioso o cualquier otro evento que pueda afectar el desempeño del sistema?
RTA	
10.	¿Cómo se lleva a cabo la realización de copias de respaldo?
RTA	
11.	¿Qué tipo de información se respalda?
RTA	
12.	¿Se ha probado la restauración de los datos? ¿Qué resultados ha arrojado dicho procedimiento?
RTA	
13.	¿Existe inventario de todos los activos de información de la KARISALUD IPS?
RTA	
14.	¿Se realiza alguna clasificación de los activos? ¿Qué criterios de clasificación se utilizan?
RTA	
15.	¿Existe un responsable de la protección de estos activos?
RTA	
16.	¿Qué procedimiento se utiliza para la eliminación de los medios de almacenamiento de información que hayan cumplido su ciclo de vida?
RTA	
17.	¿Se controla el acceso a los sistemas de información que utiliza la IPS?
RTA	
18.	¿Qué procedimientos se implementan para impedir el acceso no autorizado a los servicios red?
RTA	
19.	¿Existe un Plan de Contingencias que permita reducir el impacto en caso de pérdida de información, causada por desastres naturales, accidentes, fallas del equipo u otros eventos?
RTA	

NOMBRE DEL AUDITOR **AUDITOR**	**GERENTE** **ENTREVISTADO**

Apéndice 3. Entrevista No. 2.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT No. EN002

Empresa:	**KARISALUD IPS LTDA.**
Entrevistado:	**Gerente**

Objetivo: Evaluar el grado de cumplimiento de KARISALUD IPS en relación con el dominio de Seguridad ligada a los Recursos Humanos, contemplado en el estándar ISO 27002:2013

ÍTEM	PREGUNTA
1.	En el proceso de contratación de personal, ¿qué aspectos se tienen en cuenta para evaluar a los diferentes candidatos?
RTA	
2.	Cuando se establecen relaciones con terceros (contratistas, proveedores, etc.), ¿se hace verificación de antecedentes como requisito para la contratación?
RTA	
3.	¿Qué aspectos de los antecedentes se revisan?
RTA	
4.	¿En la etapa de contratación se establece que los empleados deben firmar un acuerdo de confidencialidad, en donde se indique la responsabilidad que tienen frente a la información a la cual van a tener acceso?
RTA	
5.	¿Se establecen acuerdos de confidencialidad con terceros?
RTA	
6.	¿Están los empleados capacitados en cuanto a la protección y manejo adecuado de la información que tienen bajo su responsabilidad?
RTA	
7.	¿Existe formalmente alguna sanción o proceso disciplinario para aquellos empleados que cometan alguna falta contra la seguridad de la información (fraude, divulgación no autorizada, pérdida de activos, entre otras)?
RTA	
8.	¿En cuánto a los derechos de acceso a información confidencial, qué procedimiento se lleva a cabo para eliminar esos derechos, cuando el empleado es retirado o movido de su cargo?
RTA	

NOMBRE DEL AUDITOR	**GERENTE**

AUDITOR	ENTREVISTADO

Apéndice 4. Entrevista No. 3.

Kari Salud I.P.S. LTDA		Universidad Francisco de Paula Santander Ocaña - Colombia
DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013		
		R/PT No. EN003
Empresa: Entrevistado:	**KARISALUD IPS LTDA.** **Gerente / Auditor**	
Objetivo: Evaluar el cumplimiento de los requisitos legales en cuanto a seguridad de la información en KARISALUD IPS LTDA.		
ÍTEM	**PREGUNTA**	
1.	¿Existe inventario de las historias clínicas de los usuarios de la Institución?	
RTA		
2.	¿Se realiza alguna clasificación de estas historias? ¿Qué criterios de clasificación se utilizan?	
RTA		
3.	¿Existe algún procedimiento establecido para la administración y protección de las historias clínicas de la IPS?	
RTA		
4.	Los acuerdos con otras instituciones que incluyen intercambio de información, ¿establecen procedimientos para identificar o interpretar las etiquetas de clasificación?	
RTA		
5.	¿Qué protocolo existe para definir el nivel de confidencialidad de la información de las historias clínicas de los usuarios?	
RTA		
6.	¿Existen formatos definidos por la IPS para registrar las solicitudes de los usuarios relacionadas con sus historias clínicas?	
NOMBRE DEL AUDITOR AUDITOR		**ENCARGADO HISTORIAS CLÍNICAS ENTREVISTADO**

Apéndice 5. Entrevista No. 4.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT No. EN004

Empresa:	**KARISALUD IPS LTDA.**
Entrevistado:	**Gerente / Auditor**

Objetivo: Evaluar el cumplimiento de los requisitos legales en cuanto a seguridad de la información en KARISALUD IPS LTDA.

ÍTEM	PREGUNTA
1.	¿El software utilizado por la IPS para el desarrollo de sus actividades, cuenta con las debidas licencias y manuales de usuario e instalación?
RTA	
2.	¿Se llevan a cabo revisiones periódicas para verificar que sólo se instale software autorizado y productos con licencia?
RTA	
3.	¿Existe un documento que contenga las políticas de seguridad de la información y de todas las repercusiones legales de la contravención de tales políticas?
RTA	
4.	¿Existen controles definidos y documentados para proteger los registros y la información de la IPS, de pérdida, destrucción y falsificación?
RTA	
5.	¿Existe alguna política de protección y privacidad de los datos personales (empleados, usuarios, proveedores, contratistas) que utiliza la Institución?
RTA	
6.	¿Estas políticas son comunicadas a las personas involucradas en el procesamiento de la información personal?

NOMBRE DEL AUDITOR AUDITOR	**GERENTE / AUDITOR ENTREVISTADO**

Apéndice 6. Lista de chequeo No. 1.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT No. LC001

Empresa: **KARISALUD IPS LTDA.**
Área o Proceso: **Infraestructura física**

Fecha Elaboración: 20/06/2016
Fecha Revisión: 24/06/2016

Objetivo: Evaluar la existencia de controles de acceso físico a las instalaciones de KARISALUD IPS.

No.	ACTIVIDAD	C	NC	R/PT	OBSERVACIONES	AUDITOR
1.	Perímetro de seguridad claramente definido					INICIALES DEL AUDITOR
2.	Área de recepción con su respectivo funcionario					
3.	Salidas de emergencia					
4.	Cámara de vigilancia en el área de recepción					
5.	Cámara de vigilancia en el área administrativa					
6.	Control de acceso al área de farmacia					
7.	Control de acceso físico al área de archivo					
8.	Control de acceso físico al área administrativa					
9.	Control de acceso al área de atención al Usuario					

MARCAS UTILIZADAS

LC001: Lista de verificación # 1
XXX.: Nombre del Auditor
C: Cumple
NC: No Cumple

Apéndice 7. Lista de Chequeo No. 2.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT LC002

Empresa: **KARISALUD IPS LTDA** | Fecha Elaboración: 22/04/2014

Área o Proceso**: Infraestructura física** | Fecha Revisión: 26/04/2014

Objetivo: Evaluar la existencia y eficacia de los controles para la protección de los equipos de cómputo.

No.	ACTIVIDAD	SI	NO	ESTADO			R/PT	NOTA	AUDITOR
				B	R	M			
1.	Alarma contra incendios								D.O.C.
2.	Detectores de humo								
3.	Extintores								
4.	UPS								
5.	Generador de emergencia (planta eléctrica)								
6.	Combustible para el generador de emergencia								
7.	Avisos de prohibiciones como fumar o comer cerca de los equipos de cómputo								
8.	Pararrayos								
9.	Sistema de refrigeración de equipos (aire acondicionado)								
10.	Impermeabilidad del techo								
11.	Impermeabilidad del piso								
12.	Protección del cableado eléctrico								
13.	Protección del cableado de datos								
14.	Independencia del cableado eléctrico y de datos								
15.	Señalización del tipo de cableado instalado								

MARCAS UTILIZADAS

LC002: Lista de Lista de verificación # 2
D.O.C.: Dina Luz Orozco Cantillo - Auditora Auxiliar
B: Bueno
R: Regular
M: Malo

Apéndice 8. Formato valoración de activos.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA001

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		
DATOS E INFORMACIÓN							
1.	documentos institucionales (Contratos, planes, proyectos)						**J.C.G.G.**
2.	Directorio de contactos						
3.	Productos institucionales (investigaciones)						
4.	Correo electrónico						
5.	Bases de datos						
6.	Historias clínicas						
7.	Información de contraseñas						
8.	Respaldos de datos (Backup)						
9.	Chat interno						
10.	Información financiera						

MARCAS UTILIZADAS

IA001: Formato Identificación de Activos No. 1
J.C.G.G.: Juan Carlos García Guarín – Auditor Principal
Valoración magnitud del daño del activo:
I: Insignificante - No causa ningún tipo de impacto o daño a la organización.
B: Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización.
M: Medio - Provoca la desarticulación de un componente de la organización.
A: Alto - En el corto plazo desarticula a la organización.

Apéndice 9. Formato valoración de amenazas.

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA002

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		
SISTEMAS E INFRAESTRUCTURA							
1.	Equipos de la red cableada (router, módem, switch,…)						**J.C.G.G.**
2.	Equipos de la red inalámbrica (router, punto de acceso,…)						
3.	Software de administración (contabilidad, citas,…)						
4.	Impresoras						
5.	Celulares						
6.	Líneas telefónicas						
7.	Computadores (de escritorio, portátiles,…)						
8.	Dispositivos de almacenamiento (USB,…)						
9.	Equipos de laboratorio						
10.	Edificación (Recepción, Sala de espera, consultorios,…)						

MARCAS UTILIZADAS

IA002: Formato Identificación de Activos No. 2
J.C.G.G.: Juan Carlos García Guarín – Auditor Principal
Valoración magnitud del daño del activo:
I: Insignificante - No causa ningún tipo de impacto o daño a la organización.
B: Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización.
M: Medio - Provoca la desarticulación de un componente de la organización.
A: Alto - En el corto plazo desarticula a la organización.

Apéndice 10. .Entrevista No. 5.

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia	
DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013	
R/PT EN005	
Empresa:	**KARISALUD IPS LTDA.**
Entrevistado:	**Usuario del sistema/módulo**
Objetivo: Verificar la implementación de los controles relacionados con la protección de la información.	
ÍTEM	**PREGUNTA**
1.	¿Qué tipo de aplicación o software utiliza?
RTA	
2.	¿Qué funciones realiza en el software que tiene a su cargo?
RTA	
3.	¿Conoce en su totalidad las funciones del software que maneja?
RTA	
4.	¿Cuánto tiempo lleva manejando el sistema?
RTA	
5.	¿Posee usted un usuario y contraseña para acceder al sistema?
RTA	
6.	¿Recibe por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?
RTA	
7.	¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?
RTA	
8.	¿Recibe usted notificación formal de los cambios de contraseñas?
RTA	
9.	¿Las funciones del sistema que no debe utilizar están restringidas?
RTA	
10.	¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?
RTA	
11.	¿En el momento de su contratación le dan a conocer las responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?
NOMBRE DEL AUDITOR AUDITOR	**USUARIO SISTEMA AUDITADO**

Apéndice 11. Lista de chequeo No. 3.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT No. LC003

Empresa: **KARISALUD IPS LTDA.**	Fecha Elaboración: 20/06/2016
Área o Proceso: **Administración de Activos**	Fecha Revisión: 24/06/2016

Objetivo: Evaluar la existencia de procedimientos establecidos por KARISALUD IPS, para la protección de sus activos de información.

No.	ACTIVIDAD	C	NC	R/PT	OBSERVACIONES	AUDITOR
1.	Inventario de activos					J.C.G.G
2.	Propietario de los activos					
3.	Políticas de uso de los activos					
4.	Clasificación de los activos					
5.	Etiquetado o codificación de los activos					
6.	Procedimientos para la seguridad de los activos					
6.	Procedimiento para la eliminación de activos					
7.	Administración de medios extraíbles (memorias USB, discos externos,…)					
8.	Procedimiento para administrar activos fuera de la empresa					

MARCAS UTILIZADAS

LC003: Lista de verificación # 3
J.C.G.G.: Juan Carlos García Guarín – Auditor Principal
C: Cumple
NC: No Cumple

Apéndice 12. Lista de chequeo No. 4.

Kari Salud I.P.S. LTDA

Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT No. LC004

Empresa: **KARISALUD IPS LTDA.**	Fecha Elaboración: 20/06/2016
Área o Proceso: **Infraestructura física**	Fecha Revisión: 24/06/2016

Objetivo: Verificar la existencia de controles para la gestión de la continuidad del negocio en KARISALUD IPS LTDA.

No.	ACTIVIDAD	C	NC	R/PT	OBSERVACIONES	AUDITOR
1.	Pólizas contra robo de equipos					D.O.C.
2.	Pólizas contra incendios					
3.	Plan de Continuidad del Negocio (PCN)					
4.	Plan de Contingencias					
5.	Contacto con autoridades					
5.1	*Bomberos*					
5.2	*Cruz Roja*					
5.3	*Policía Nacional*					
5.4	*Aseguradoras*					
5.5	*Grupos de interés*					
6.	Servicio de Data Center					
7.	Respaldos de información fuera de las instalaciones de la IPS					
8.	Instalaciones alternas					

MARCAS UTILIZADAS

LC004: Lista de verificación # 4
D.O.C.: Dina Luz Orozco Cantillo – Auditora Auxiliar
C: Cumple
NC: No Cumple

Apéndice 13 .Formato valoración de activos No. 3.

Kari Salud I.P.S. LTDA — Universidad Francisco de Paula Santander Ocaña - Colombia

DISEÑO DE UNA GUÍA DE APLICABILIDAD DE CONTROLES DE SEGURIDAD PARA LA IPS KARISALUD LTDA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013

R/PT IA003

Empresa: **KARISALUD IPS LTDA**

Fecha Elaboración: 22/04/2014
Fecha Revisión: 26/04/2014

Objetivo: Identificar los activos o elementos de información de KARISALUD IPS.

No.	ACTIVIDAD	MAGNITUD DAÑO				OBSERVACIONES	AUDITOR
		I	B	M	A		
PERSONAL							
1.	Junta Directiva						**D.O.C.**
2.	Gerencia						
3.	Auditoría						
4.	Atención al usuario						
5.	Personal técnico						
6.	Personal informático interno						
7.	Personal informático externo						
8.	Soporte técnico interno						
9.	Soporte técnico externo						
10.	Personal de limpieza/interno						
11.	Servicio de mensajería/propio						
12.	Servicio de mensajería externo						
13.	Vigilancia privada						

MARCAS UTILIZADAS

IA003: Formato Identificación de Activos No. 3
D.O.C.: Dina Luz Orozco Cantillo – Auditora Auxiliar
Valoración magnitud del daño del activo:
I: Insignificante - No causa ningún tipo de impacto o daño a la organización.
B: Bajo - Causa daño aislado, que no perjudica a ningún componente de la organización.
M: Medio - Provoca la desarticulación de un componente de la organización.
A: Alto - En el corto plazo desarticula a la organización.