PROYECCIÓN FINANCIERA Y TECNOLÓGICA REQUERIDA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), BAJO LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA INDAIRE INGENIERÍA S.A.S.

OSCAR JAVIER ZAQUE GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2016

PROYECCIÓN FINANCIERA Y TECNOLÓGICA REQUERIDA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), BAJO LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA INDAIRE INGENIERÍA S.A.S.

OSCAR JAVIER ZAQUE GONZÁLEZ

Para optar al título de Especialista en Seguridad Informática.

Director de Proyecto

Ingeniero John Quintero

Esp. Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2016

NOTA DE ACEPCTACIÓN

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Fecha

DEDICATORIA

Dedico esta tesis a mi esposa quien estuvo a mi lado durante todo el proceso, apoyándome de manera significativa en el tiempo que tomo la elaboración de esta especialización.

AGRADECIMIENTOS

Agradezco a Dios por la oportunidad de lograr culminar este nuevo proyecto de manera exitosa, a mi esposa quien fue mi bastón y me acompaño durante todo el camino. Igualmente agradezco a la UNAD, al equipo docente y de especialistas quienes con su profesionalismo, experiencia y calidad humana guiaron este desarrollo.

CONTENIDO

Página

CONTENIDO....6
1. INTRODUCCIÓN.... 11
2. PREGUNTA PROBLEMA.... 12
3. PLANTEAMIENTO DEL PROBLEMA.... 13
4. JUSTIFICACIÓN.... 14
5. OBJETIVOS.... 15
5.1. OBJETIVO GENERAL.... 15
5.2. OBJETIVOS ESPECÍFICOS.... 15
6. MARCO CONTEXTUAL.... 16
6.1. MISIÓN.... 16
6.2. VISIÓN.... 16
6.3. ORGANIGRAMA.... 16
6.4. LOCALIZACIÓN GEOGRÁFICA.... 17
7. MARCO REFERENCIAL.... 19
7.1. MARCO TEÓRICO.... 21
7.1.1. Seguridad informática.... 21
7.1.2. Evaluación de activos.... 22
7.1.3. Evaluación de riesgos informáticos.... 23
8. MARCO LEGAL.... 27
9. DISEÑO METODOLÓGICO.... 28
9.1. ALCANCE DEL PROYECTO.... 28
9.2. MÉTODOS PARA LA BÚSQUEDA DE INFORMACIÓN.... 28
9.2.1. Identificación de los Activos de la Empresa.... 28
9.2.2. Análisis de vulnerabilidades.... 30
9.2.3. Identificación de requerimientos de seguridad para la compañía.... 31

9.2.4. Costos de implementación del sgsi en la empresa Indaire ingeniería s.a.s. 32
10. DESARROLLO DEL PROYECTO 34
10.1. IDENTIFICACIÓN DE LOS ACTIVOS DE LA EMPRESA. 34
10.1.1. Dependencia entre Activos. 40
10.2. ANÁLISIS DE VULNERABILIDADES. 41
10.2.1. Identificación de acceso y puertos abiertos 41
10.2.2. Verificación de redes inalámbricas y accesos web. 43
10.2.3. Análisis de vulnerabilidades físicas a activos tecnológicos. 46
10.2.4. Matriz de vulnerabilidades. 48
10.3. IDENTIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD PARA LA COMPAÑÍA. 51
10.3.1. Obtener el Apoyo de la Dirección. 52
10.3.2. Definición de alcance. 52
10.3.3. Redacción de las políticas de seguridad. 52
10.3.4. Definición de la Metodología de evaluación de riesgos, Evaluación de riesgos y tratamiento de riesgos. 52
10.3.5. Redacción de la Declaración de Aplicabilidad y el plan de tratamientos. 54
10.3.6. Implementación de Programas de Capacitación y Concientización. 54
10.3.7. Puesta en Marcha del SGSI. 55
10.3.8. Supervisión del SGSI por medio de Auditoría Interna Periódica 55
10.3.9. Revisión por parte de la dirección. 55
10.3.10. Certificación Icontec 55
10.4. COSTOS DE IMPLEMENTACIÓN DEL SGSI EN LA EMPRESA INDAIRE INGENIERÍA S.A.S. 55
11. CONCLUSIONES 57
12. BIBLIOGRAFÍA 58
13. ANEXOS 60

LISTA DE TABLAS

Página

Tabla 1. Escala de Valoración Cualitativa de Probabilidad de Ocurrencia de un Incidente o Amenaza. 24
Tabla 2. Escala de Valoración Cuantitativa de Probabilidad de Ocurrencia de un Incidente o Amenaza. 25
Tabla 3. Normativa legal aplicable al SGSI en Colombia. 27
Tabla 4. Escala de valoración cualitativa de activos. 29
Tabla 5. Escala de valoración cuantitativa de activos. 29
Tabla 6. Matriz de identificación de activos tecnológicos. 36
Tabla 7. IP Encontradas en la red. 41
Tabla 8. Identificación de puertos abiertos. 42
Tabla 9. Escala de Valoración de Vulnerabilidades físicos a activos tecnológicos 47
Tabla 10. Análisis de Vulnerabilidades físicas de activos tecnológicos. 47
Tabla 11. Identificación del Riesgo. 48
Tabla 12. Matriz de Riesgos. 51
Tabla 13. Recomendaciones de protección para la compañía. 53
Tabla 14. Proyección Financiera SGSI Indaire Ingeniería S.A.S. 63

TABLA DE FIGURAS

Página.

Figura 1. Organigrama Indaire Ingeniería S.A.S 17
Figura 2. Localización geográfica Indaire Ingeniería S.A.S. 18
Figura 3. Controles de seguridad de riesgos y amenazas informáticos. 22
Figura 4. El riesgo en función del impacto y la probabilidad. 26
Figura 5. Fotografía de la oficina Indaire Ingeniería s.a.s. 34
Figura 6. Sistemas de aire acondicionado. 35
Figura 7. Equipos y personal de oficina. 35
Figura 8. Tablero de Control 35
Figura 9. Componentes del aire acondicionado. 35
Figura 10. Árbol de dependencia entre Activos. 40
Figura 11. Identificación de dispositivos conectados a la red. 42
Figura 12. Configuración de la red LAN. 43
Figura 13. Configuración del router. 44
Figura 14. Análisis con Acrylic Wifi 45
Figura 15. Características internas de la red Wi-fi de Indaire Ingeniería s.a.s 46
Figura 16. Escaneo de puertos 192.168.1.101 61
Figura 17. Escaneo de puertos IP192.168.1.100 61
Figura 18. Escaneo de puertos IP192.168.1.105 61
Figura 19. Escaneo de puertos IP192.168.1.106 62
Figura 20. Escaneo de puertos IP192.168.1.113 62
Figura 21. Escaneo de puertos IP192.168.1.117 62

TABLA DE ANEXOS

Página

Anexo 1. Carta de aprobación de la compañía. 60
Anexo 2. Pantallazos Análisis de Puertos Abiertos de cada IPcontenida en la Red, mediante la herramienta Nmap..... 61
Anexo. 3 Proyección Financiera SGSI para la compañía Indaire Ingeniería S.A.S..... 63
Anexo. 4. Cotizaciones recomendaciones físicas (Control de acceso y CCTV)..... 65
Anexo. 5 Cotizaciones recomendaciones físicas (UPS y Detector de humo c/u). 66

1. INTRODUCCIÓN

Los ciberataques son la modalidad delictiva más común a la que se ven expuestas diariamente las compañías colombianas, vulnerando el activo más valioso de las mismas: la información.

Aunque Colombia es el único país en Latinoamérica que tiene un plan de lucha contra el ciber - crimen según datos consolidados por la corporación Colombia digital, los casos continúan en aumento y cada vez resulta más complicado detectar los ataques a los que constantemente se ven expuestas las compañías nacionales. Debido a esto las empresas actualmente se ven obligadas a destinar tiempo y fondos para la implementación de sistemas de seguridad informáticos que permitan conocer las vulnerabilidades existentes con el fin de minimizarlas o evitarlas para así lograr proteger la información y los datos sensibles de la compañía.

En el presente proyecto se analizan los niveles de seguridad de la información existentes dentro de la compañía Indaire Ingeniería. Los análisis elaborados dentro de la empresa Indaire Ingeniería S.A.S analizan el software y hardware existente dentro de la empresa para poder determinar las brechas de seguridad existentes ya sea por medios físicos o virtuales. La seguridad física la determinamos por medio de una inspección de los niveles de acceso a los servidores así como a los equipos de cómputo, de esta manera podemos conocer las necesidades de seguridad y que tan viable sería realizar una extracción de información de las instalaciones de la empresa.

Por otro lado el análisis de software sugiere una serie de pruebas de redes así como un sondeo del estado de los puertos por los cuales podrían realizarse infiltraciones de cualquier tipo, estas pruebas se realizan realizando hacking ético a las redes internas y de esta manera poder determinar si los elementos existentes tales como el antivirus o firewall son suficiente protección para los datos contenidos en los equipos.

Al analizar y determinar las vulnerabilidades y brechas de seguridad existentes dentro de la red se determinan los elementos de protección que se requieren para mantener un nivel de seguridad óptimo. Con este fin se realiza una proyección financiera para la implementación de un SGSI en base a algunas recomendaciones y cotizaciones elaboradas por el equipo de trabajo.

La implementación del SGSI será decisión de la gerencia de la compañía por lo cual se entrega un informe completo el cual contiene los costos y tiempos de implementación de cada una de las fases.

2. PREGUNTA PROBLEMA

¿Cuáles son los requerimientos financieros y tecnológicos necesarios para la implementación del Sistema de Gestión de la Seguridad de la Información, en la empresa Indaire Ingeniería S.A.S.?

3. PLANTEAMIENTO DEL PROBLEMA

Indaire Ingeniería S.A.S, es una empresa privada especializada en las áreas de acondicionamiento de aire (Comercial, industrial, Hospitalario y de precisión para los centros de datos y centrales de comunicaciones). El uso de la red informática no se encuentra reglamentado ni cuenta con protección alguna, también existe la necesidad de compartir datos e información entre los usuarios e interesados poniendo en riesgo la seguridad interna de la red, permitiendo el acceso no deseado de terceros y generando posibles intrusiones.

Debido a que Indaire Ingeniería S.A.S. no cuenta con un sistema de seguridad de la información implementado, los activos y la información de la empresa se encuentran en constante riesgo. Esta situación perjudica notablemente la seguridad de los datos gerenciales, financieros y operacionales de la organización. Dicha situación desmejora la rentabilidad de la compañía frente al mercado existente y la expone a espionaje y pérdida de clientes.

En aras de solucionar esta problemática la empresa debe implementar una solución hacia la Gestión de la Seguridad de la Información, de acuerdo a los objetivos del negocio, por ello se hace necesario realizar una proyección financiera para la implementación de un SGSI en la organización, que permita identificar si la compañía Indaire Ingeniería S.A.S. puede sostener e implementar dicho sistema y de esta manera lograr optimizar las inversiones realizadas en controles que protejan los activos.

4. JUSTIFICACIÓN

El presente proyecto pretende realizar la proyección financiera y tecnológica para que la empresa Indaire Ingeniería S.A.S. implemente su Sistema de Gestión de la Seguridad de la Información, este con el fin conseguir niveles de seguridad mínimos para la compañía.

La proyección incluye todos los aspectos económicos, financieros y tecnológicos requeridos para la implementación de los controles de seguridad planteados en la normativa ISO/IEC 27001:2013, de manera que garantice la operatividad del sistema y el sostenimiento del mismo, bajo el enfoque de mejora continua.

Con este proyecto se busca que la empresa Indaire Ingeniería S.A.S. conozca las posibles amenazas actuales y futuras a las que se encuentra expuesta, la normativa vigente ante las amenazas y la necesidad de un SGSI que aporte políticas de seguridad actualizadas para obtener buenas prácticas dentro de la organización y así garantizar la protección continua de la información interna y externa de la compañía.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Crear la proyección financiera y de recursos tecnológicos requeridos para la implementación del sistema de gestión de la seguridad de la información (SGSI), bajo la norma ISO/IEC 27001:2013 en la empresa Indaire Ingeniería S.A.S, esta como herramienta para que le permita a las directivas determinar la factibilidad del sistema y tomar decisiones sobre el desarrollo, aplicación y sostenibilidad del mismo.

5.2. OBJETIVOS ESPECÍFICOS

- Realizar la identificación de activos tecnológicos y de negocio en la compañía mediante una matriz de identificación.
- Realizar el análisis de vulnerabilidades y amenazas existentes en los sistemas informáticos con el fin de encontrar posibles fallas de seguridad en el sistema interno de la compañía.
- Presentar los controles, medidas y recursos necesarios requeridos para determinar los costos de implementación.
- Determinar la proyección económica de la implementación del SGSI para Indaire ingeniería S.A.S.

6. MARCO CONTEXTUAL

Indaire Ingeniería S.A.S. Es una compañía en el mercado Colombiano dedicada al diseño, comercialización, montaje, mantenimiento y asesoría profesional para la selección y expansión de sistemas de aire acondicionado, equipos de control ambiental, ventilación mecánica, automatización de edificios y seguridad a nivel nacional., fundada y dirigida por el ingeniero Mecánico Carlos Donoso desde hace 8 años.

6.1. MISIÓN

Generamos calidad de vida por medio de soluciones tecnológicas ofreciendo servicios de ingeniería y asesoría profesional para la selección, diseño y expansión de sistemas con equipos de control ambiental, ventilación mecánica, a nivel nacional. Contando con personal idóneo y altamente calificado fundado en valores éticos motivado y comprometido a trabajar por la satisfacción de nuestros clientes, proveedores y la sociedad en general.

6.2. VISIÓN

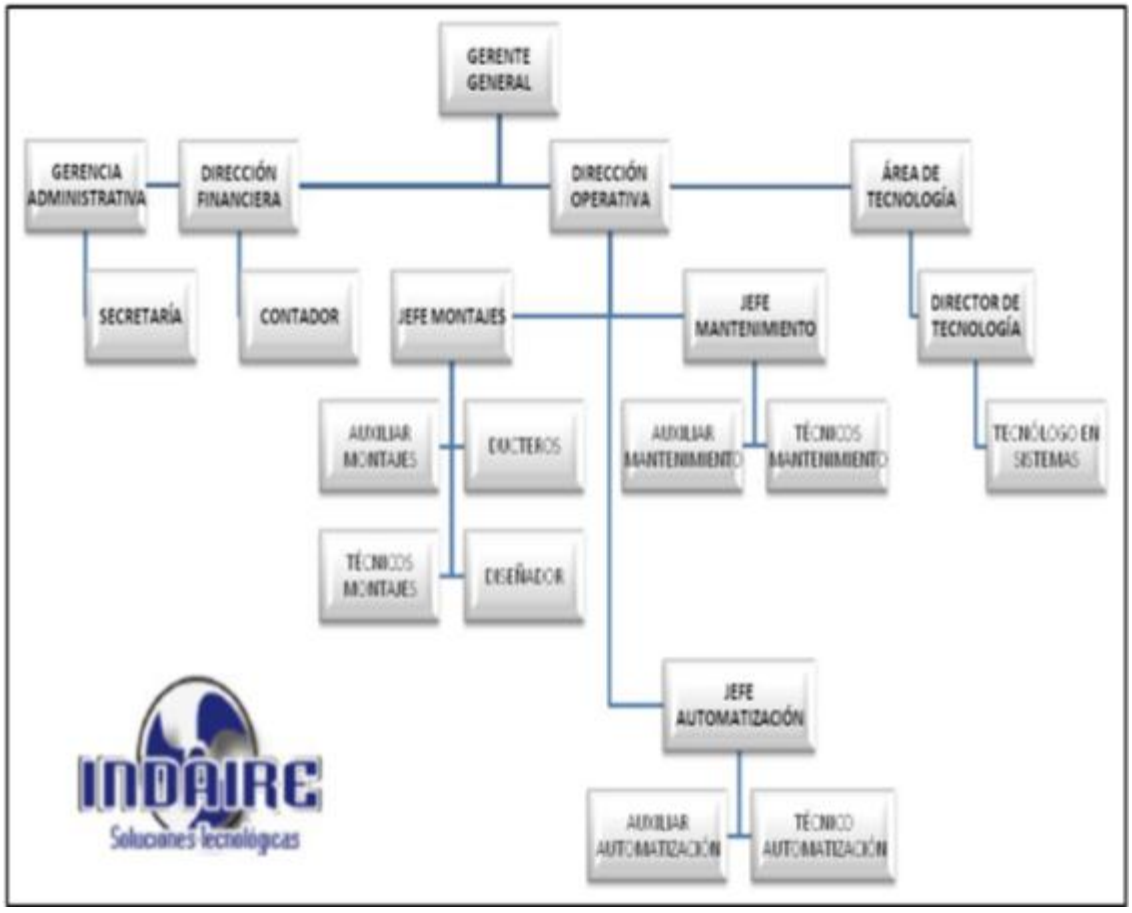
INDAIRE INGENIERIA S.A.S. en el año 2017 será la empresa preferida en la prestación de servicios de acondicionamiento de aire y control ambiental a nivel nacional. Seremos una organización eficaz y eficiente soportada en innovación, servicio y calidad.

Seremos generadores de empleo recalcando siempre el recurso humano como lo más valioso.

6.3. ORGANIGRAMA

La estructura organizacional de la compañía Indaire ingeniería inicia con el gerencia y de ahí se despliegan las demás dependencias que se encuentran en la compañía como lo son el área administrativa, dirección financiera, dirección operativa y área tecnológica en la figura 1 se muestra el organigrama general de la compañía.

Figura 1. Organigrama Indaire Ingeniería S.A.S

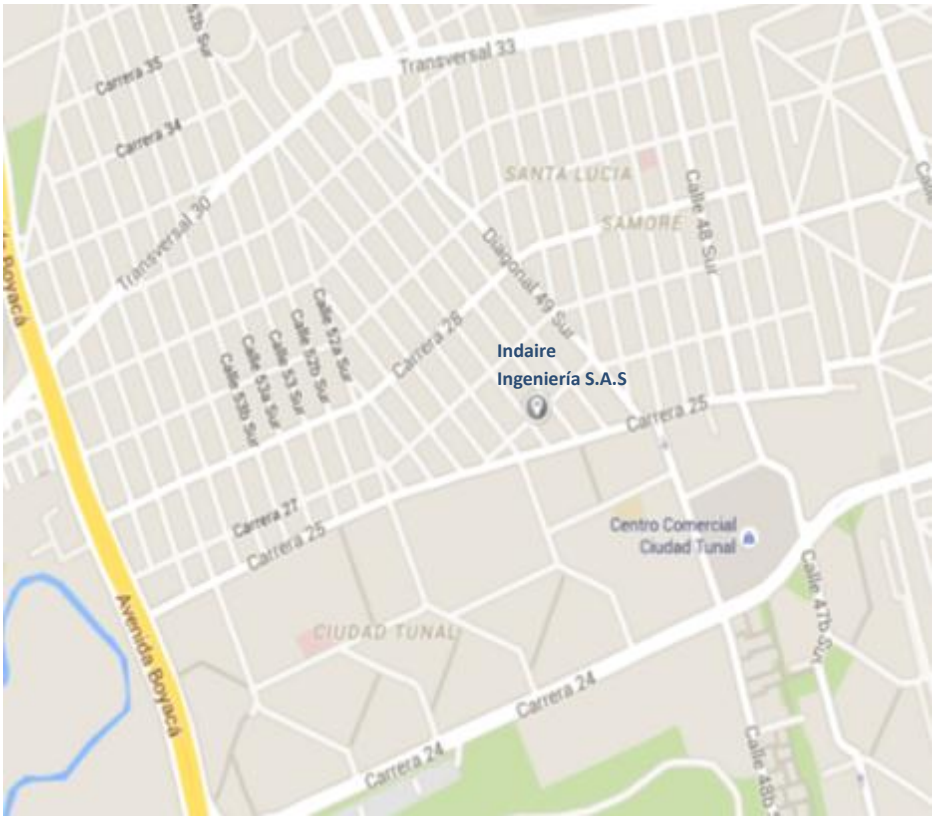


Fuente. Indaire Ingeniería S.A.S

6.4. LOCALIZACIÓN GEOGRÁFICA.

La sede principal de la compañía Indaire Ingeniería s.a.s se ubica en el centro del país en la ciudad de Bogotá, localidad N° 6 de Tunjuelito en la UPZ 62 Venecia Barrio el Tunal. En la figura 2 se detalla en una imagen de google maps la localización de la compañía.

Figura 2. Localización geográfica Indaire Ingeniería S.A.S.



Fuente. Google maps 2015.

7. MARCO REFERENCIAL

La información en una compañía como lo dice Martha Landino en su artículo Fundamentos de Iso 27001 y su Aplicación en las Empresas, es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento del uso de internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques, ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad. (p.334)[1]

Por ello se hace necesario proteger la información financiera, activos y demás de la compañía como de los clientes de la misma usando mecanismos que le permitan a la compañía verificar de forma eficaz el estado de sus activos tecnológicos y en caso de estar vulnerados o amenazados los controles pertinentes, para evitar infiltraciones a sus sistemas se crearon herramientas de protección informática como lo son los sistemas de gestión de la seguridad informática (SGSI).

Un Sistema de Gestión de la Seguridad Informática SGSI, como lo dice Diana Calderón (2011) "Se encarga de la protección de los activos de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales". (p.21)[2]

Entonces se dice que un SGSI es un "conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware"[3] que le permiten a la compañía controlar el riesgo y proteger su información de forma adecuada sin afectar sus procesos. El SGSI en la compañía se enfoca en mantener la estabilidad en confiabilidad (Acceso a los activos únicamente por personal autorizado), integridad (Exactitud de la información) y Disponibilidad (Acceso a la información por el personal autorizado cuando este lo requiera).

[1] Scientia et Technica Año XVII, No 47, Abril de 2011. Universidad Tecnológica de Pereira. ISSN 0122-1701.(p.334)

[2] CALDERON DIANA. Implementación de sistema de gestión de seguridad de la información aplicada al área de recursos humanos de la empresa decevale s.a. Escuela Superior Politécnica del Litoral. Guayaquil, 2011. p.21.

[3] Ibíd., p. 21

Las organizaciones ISO e IEC se encargaron de desarrollar la serie de estándares ISO/IEC 27000 con el fin de normalizar los procedimientos y protocolos para la creación de sistemas de gestión de la seguridad informática en cualquier tipo de organización. La serie 27000 está compuesta por normas como: BS 7799-1 1995 de BS la cual es un conjunto de buenas prácticas para la gestión de la seguridad de una compañía, BS 7799-2 1998 de BS en esta se establecen una serie de apartados para la construcción de un SGSI certificable por una organización independiente.

La primera publicación de la serie de estándares ISO/ IEC 27000 se realizó en el año 2005 luego de realizarle revisiones a las normas que la contienen. En el mismo año se le realiza algunas correcciones al estándar inicial y se publica la norma ISO/IEC 27001 la cual tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de la información de una organización, por lo tanto se establecen parámetros claros para la gestión del riesgo entre estos parámetros están[4]:

- Definición del alcance del SGSI
- Redacción de la política de seguridad.
- Definición de la Metodología de evaluación de riesgos, Evaluación de riesgos y tratamiento de riesgos.
- Redacción de la Declaración de Aplicabilidad y el plan de tratamientos.
- Implementación de Programas de Capacitación y Concientización.
- Puesta en Marcha del SGSI.
- Supervisión del SGSI por medio de Auditoría Interna Periódica.
- Revisión por parte de la dirección.
- Certificación

Una empresa que quiera implementar un SGSI primero debe analizar si económicamente puede asumirlo; el mecanismo para realizar ese análisis son las proyecciones financieras. La proyección financiera permite conocer el costo de implementación del sistema de gestión de seguridad informática, también analiza e identifica si la empresa cuenta con la capacidad económica de implementar y sostener el SGSI.

Las proyecciones financieras de acuerdo a la comunidad de Madrid[5], deben demostrar fiabilidad, estabilidad del sistema ante la gerencia de la compañía, en dado caso que la compañía no tenga la capacidad financiera requerida para la

[4] Ibíd., p. 21

[5]COMUNIDAD DE MADRID, ÁREA DE ANÁLISIS DE RIESGOS. Proyecciones Financieras. Plan de formación Comunidad de Madrid documento electrónico. [Citado el 13-05-2015], pp. 1. Habilitado en: http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/proyecciones_financieras_es.pdf.

implementación del sistema, la proyección demuestra si la empresa tiene la capacidad de endeudamiento para la implementación del SGSI. Según el Entrepreneur[6], en el artículo "*Aprende a hacer proyecciones financieras*" para realizar una proyección financiera se debe definir:

- El tiempo de proyección con el fin de evaluar metas periódicamente.
- Se debe elaborar un estado de resultados en el que se analizan aspectos como ingresos, egresos y costos del programa.
- Se realiza el histórico de ventas de la empresa para así determinar los ingresos de la compañía.
- Se evalúan los costos de implementación y mantenimiento del sistema, con estos se determina si realmente para la compañía es positivo poner en marcha el SGSI.

7.1. MARCO TEÓRICO

7.1.1. Seguridad informática.

Según Luis Patiño en su *Propuesta de Actualización y Aplicación de Políticas de Seguridad Informática en una Empresa Corporativa Propolsinecor* la seguridad informática se entiende como la aceptación clara de cada uno de los usuarios del sistema informático de la compañía, en conocer las PSI, herramienta que permite adoptar una cultura de seguridad, orientado a proteger el activo informático y estratégico de la compañía, los cuales deben estar alineados con los objetivos del negocio y los criterios de seguridad considerados por El Información Technology Evaluation Criteria[7].

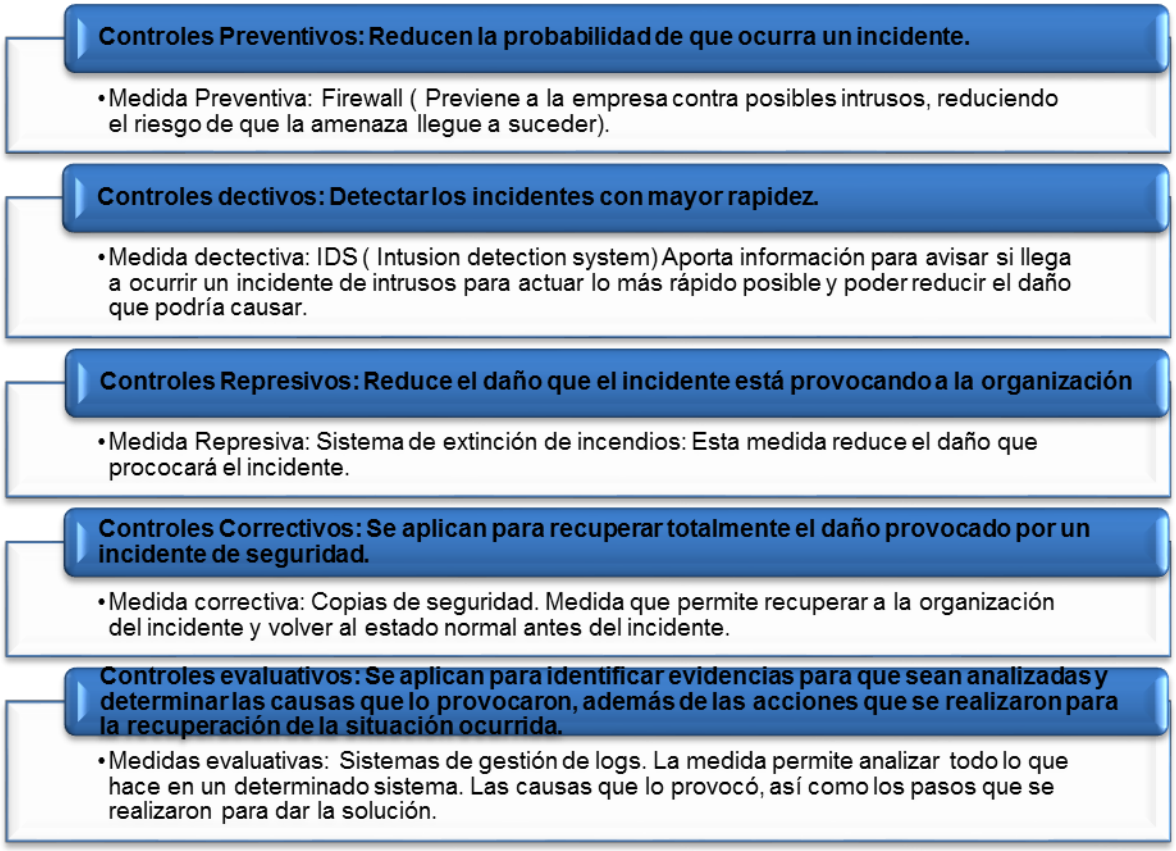
La seguridad informática busca minimizar los riesgos a los que se encuentran los bienes y servicios de una compañía mediante técnicas y procedimientos seguros para la gestión del riesgo. Para gestionar el riesgo de manera adecuada es necesario realizar un estudio de los activos con los que cuenta la compañía, el riesgo o amenazas a los que se encuentra expuesto y el posible tratamiento de los riesgos.

Según Daniel Cruz en Gestión de la seguridad de la información. Existen diferentes tipos de controles de seguridad pueden ser preventivos, dectivos, represivos, correctivos o evaluativos y se describen en la figura N° 3.

[6] REVISTA ENTREPRENEUR [En línea], Aprende a hacer proyecciones financieras. [Citado el 13-05-2015], pp. 1-2. Habilitado en: http://www.soyentrepreneur.com/aprende-a-hacer-proyecciones-financieras.html.

[7] PATIÑO, Luis Olmedo. Propuesta de actualización y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor. Tesis Especialista en Seguridad Informática. Sanjuán de Pasto: Universidad Nacional Abierta y a Distancia. Escuela de ciencias Básicas, Tecnología e ingeniería. 2014. Pg. 22.

Figura 3. Controles de seguridad de riesgos y amenazas informáticos.



Fuente: Daniel cruz Allende. (2006). Gestión de la Seguridad de la Información. Universidad Abierta de Cataluña – UOC.

7.1.2. Evaluación de activos

La evaluación de los activos es parte fundamental para realizar la identificación de los riesgos existentes en la compañía de forma correcta. De acuerdo a la oficina asesora de sistemas de la Universidad Distrital Francisco José de Caldas la identificación de los activos se debe realizar con el siguiente procedimiento[8]:

1. Realizar un inventario de activos: El inventario de activos permite identificar los activos tecnológicos con los que cuenta la compañía.

   En el inventario de activos se debe incluir el tipo de activo que se está identificando, la fecha de inventariado, estado físico en el que se encuentra el activo y su función dentro de los procedimientos de la organización.

[8] OFICINA ASESORA DE SISTEMAS UDFJC, Capítulo 5 Gestión del Riesgo. pg. 9.

2. Identificación de la relevancia de los activos: Se entiende como relevancia "los puntos claves a considerar durante la realización del análisis de riesgos. Dicha relevancia será de gran importancia para identificar el rumbo de las acciones del plan de Riesgos"[9].

3. Valoración de los activos: para la correcta identificación de la relevancia de los riesgos se deben tener valoraciones tanto cualitativas como cuantitativas de los activos. La escala de valoración cualitativa de activos se da de acuerdo a la importancia que tiene el activo para el proceso productivo de la compañía. La escala valoración cualitativa puede darse desde muy bajo hasta muy alto.

   La escala de valoración cuantitativa se determina de acuerdo al valor monetario del activo para la compañía. De igual forma la escala de valoración cuantitativa se da desde muy bajo hasta muy alto. A cada una de las valoraciones se les da una calificación y la ponderación de las dos será la valoración final de cada activo.

7.1.3. Evaluación de riesgos informáticos

La evaluación de los riesgos es parte fundamental para los sistemas de gestión de la seguridad de la información ya que a partir de esta se puede identificar el estado de seguridad en el que se encuentra la compañía y los procedimientos a seguir para mitigar el riesgo. Una de las metodologías más usadas para la valoración del riesgo es la MAGERIT. (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). La cuál es elaborada por el Consejo superior de administración electrónica de España. Esta metodología ofrece procedimientos para el análisis de los riesgos derivados del uso de las tecnologías de la información.

La metodología MAGERIT contempla el análisis de los riesgos y el tratamiento de los mismos. Su objetivo principal es concientizar a las organizaciones sobre el riesgo de infiltración o pérdida de sus activos y la debida gestión del riesgo.

Para poder realizar la debida gestión del riesgo inicialmente se debe realizar la valoración de activos la cual se explicó en el numeral anterior y se deben identificar las dependencias entre los mismos. Según MAGERIT los activos superiores tienen dependencias con activos inferiores ya sean servicios, productos, hardware, software, etc.

[9] Ibíd. Pg. 9

7.1.3.1. Determinación de amenazas

MAGERIT define amenaza como son “cosas que ocurren”, es todo lo que puede ocurrirle o pasarle a los activos y además puede causar un daño. UNE 1504:2008 define una amenaza como “*causa potencial de un incidente que puede causar daños a un sistema de información o a una organización”.*[10]

Según MAGERIT las amenazas típicas que pueden afectar uno o varios activos de una organización son las siguientes:

- **De origen natural:** Hay accidentes naturales (terremotos, inundaciones,...). Ante esos avatares el sistema • de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
- **Del entorno (de origen industrial):** Hay desastres industriales (contaminación, fallos eléctricos,...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
- **Defectos de las aplicaciones:** Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades.
- **Causadas por las personas de forma accidental**: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- **Causadas por las personas de forma deliberada:** Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Cuando se ha identificado el tipo de amenaza que puede afectar al activo se procede a determinar la degradación, es decir se determina el nivel de daño que puede sufrir el activo por la amenaza y la probabilidad de ocurrencia de la amenaza sobre el activo. La probabilidad de ocurrencia se puede valorar de forma cualitativa y cuantitativa, en las tablas 1 y 2 se refleja las escalas de valoración de acuerdo a MAGERIT.

Tabla 1. Escala de Valoración Cualitativa de Probabilidad de Ocurrencia de un Incidente o Amenaza.

[10] CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.27.

MA	Muy Alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente. CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.28.

Tabla 2. Escala de Valoración Cuantitativa de Probabilidad de Ocurrencia de un Incidente o Amenaza.

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente. CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.28.

En la escala de valoración cuantitativa según MAGERIT la frecuencia de ocurrencia de referencia es 1 año para así determinar una tasa anual de ocurrencia de amenazas.

7.1.3.2. Determinación del Riesgo.

Magerit determina el riesgo como "la medida probable de un daño sobre un sistema"[11]. El riesgo puede crecer o disminuir de acuerdo al impacto y probabilidad de ocurrencia sobre el activo, por lo tanto según magerit para evaluar el riesgo se dan cuatro zonas:

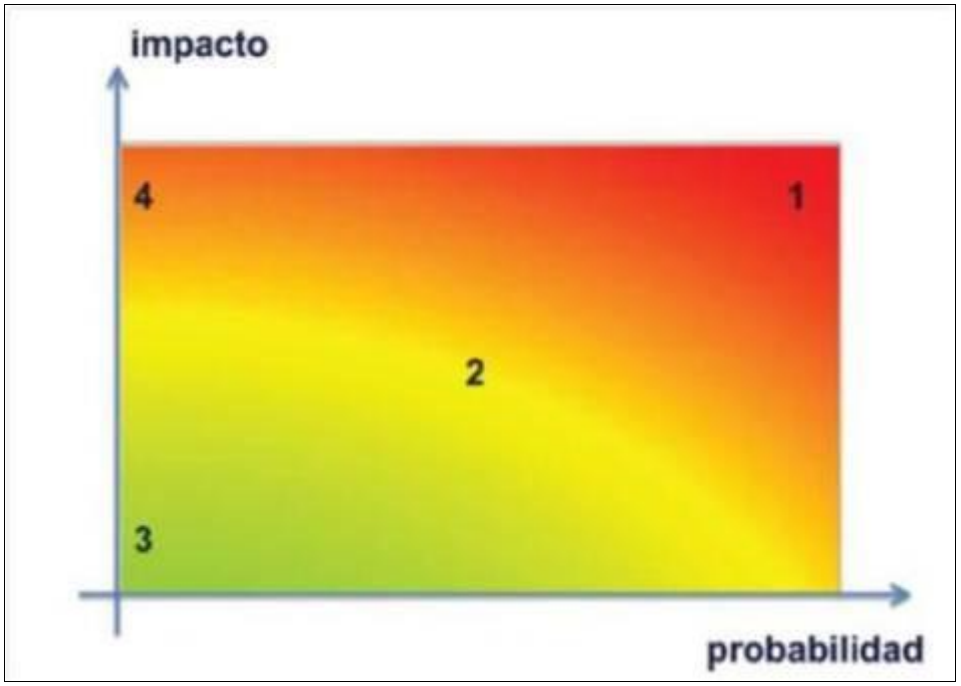
- **Zona 1:** riesgos muy probables y de muy alto impacto
- **Zona 2:** franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo

[11] Ibíd. Pg. 29

- **Zona 3**: riesgos improbables y de bajo impacto
- **Zona 4**: riesgos improbables pero de muy alto impacto

En la figura 4 se muestra la valoración del riesgo en función del impacto y la probabilidad de acuerdo a MAGERIT.

Figura 4. El riesgo en función del impacto y la probabilidad.



Fuente. CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.28.

Al realizar la ponderación de los valores identificados de riesgos y amenazas de cada activo se determina el estado general de la organización en cuanto a riesgos y los controles a implementar para mitigar el riesgo al que se ve afectada la compañía.

8. MARCO LEGAL

Este proyecto se enmarca bajo normativa legal vigente en Colombia para los sistemas de gestión de la seguridad informática. A continuación en la tabla 3 se presenta la normativa y su aplicación en el proyecto.

Tabla 3. Normativa legal aplicable al SGSI en Colombia.

NORMA	ENTIDAD	DESCRIPCIÓN
Ley 603 de 2000	Congreso de la República de Colombia	Define disposiciones sobre la protección a los derechos de autor en Colombia. Teniendo en cuenta que un software es un activo que se encuentra protegido por los derechos de autor.
Ley 1266 de 2008	Congreso de la República de Colombia	Define disposiciones sobre el habeas data, información contenida en bases de datos ya sea financiera, crediticia, comercial o de servicios.
Ley 1273 de 2009	Congreso de la República de Colombia	Se modifica el código penal y se crea la protección de la información y de los datos como bien jurídico. Se establece que se deben proteger los sistemas que usen tecnologías de la información y las comunicaciones. También define disposiciones sobre los atentados a los bienes informáticos y otras infracciones de este tipo.
Ley 1581 de 2012	Congreso de la República de Colombia	Se establece el régimen general de la protección de los datos personales. Se reglamenta que cada empresa debe establecer políticas de seguridad de la información y establecer procedimientos adecuados para atención de peticiones, quejas y reclamos.
Decreto 1377 de 2013	Presidencia de la República de Colombia	Se reglamenta parcialmente la ley 1581 de 2012 y se hacen algunas modificaciones en cuanto a las autorizaciones para el uso y tratamiento de la información personal.

Fuente: Autor

9. DISEÑO METODOLÓGICO.

Esta etapa del proyecto evidencia el tipo de investigación que se efectúa, las herramientas y procedimientos para el desarrollo de la proyección financiera y tecnológica requerida para la implementación del sistema de gestión de la seguridad de la información (sgsi), bajo la norma Iso/iec 27001:2013 en la empresa Indaire ingeniería s.a.s.

9.1. ALCANCE DEL PROYECTO

Indaire Ingeniería S.A.S. es una compañía dedicada al diseño, instalación y mantenimiento de aire acondicionado para hogares, edificios y empresas. Indaire Ingeniería cuenta con una infraestructura tecnológica operada desde una única oficina, en ella funcionan entre 6 y 7 computadores, cada uno de ellos hace uso de recursos compartidos como internet, impresora, recursos ofimáticos, software contable y de diseño.

La compañía cuenta con un servicio de internet de 3 megas el cual se reparte en todos los usuarios de la oficina. De acuerdo a lo anterior se busca cumplir los objetivos del proyecto de forma descriptiva de los procesos para llevar a cabo la proyección financiera del SGSI para la empresa Indaire Ingeniería S.A.S.

9.2. MÉTODOS PARA LA BÚSQUEDA DE INFORMACIÓN

Para la proyección financiera y tecnológica del SGSI en la empresa Indaire Ingeniería S.A.S se implementa la siguiente metodología:

9.2.1. Identificación de los Activos de la Empresa.

Esta primera etapa se inicia con el personal de la compañía que aporte información acerca de los activos y de los procesos productivos y financieros en los que sea de vital importancia la seguridad de la información contenida. También se debe realizar una clasificación de activos de acuerdo a su nivel de importancia y confidencialidad teniendo en cuenta los procesos productivos y financieros mediante una matriz de identificación que se describe a continuación.

9.2.1.1. Matriz de identificación de activos tecnológicos.

Esta identificación se realiza teniendo en cuenta cada uno de los recursos físicos y virtuales existentes en la compañía, en esta también se evalúa el estado físico en el que se encuentra el activo, su función dentro del proceso productivo en la empresa y el porcentaje de cumplimiento del mismo. De igual manera se analizaran los activos según su importancia ya sea crítica, media o leve dentro del proceso y la información contenida en ellos.

Se usan dos escalas de valoración de activos cualitativa y cuantitativa. La escala de valoración cualitativa se determina teniendo en cuenta la importancia del activo dentro del proceso de la compañía. La escala de valoración cuantitativa se determina teniendo en cuenta el valor monetario del activo. Las escalas de valoración cualitativa y cuantitativa se muestran en las tablas 4 y 5.

Tabla 4. Escala de valoración cualitativa de activos.

Escala de Valoración	Color de Escala Valorativa	Valor	Descripción
MB: Muy Bajo		1	Irrelevante para efectos prácticos
B: Bajo		2	Importancia menor para el desarrollo del proyecto
M: Medio		3	Importante para el proyecto
A: Alto		4	Altamente importante para el proyecto
MA: Muy alto		5	De vital importancia para los objetivos que persigue el proyecto

Fuente**.** MAGERIT- Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 5. Escala de valoración cuantitativa de activos.

Escala de Valoración	Color de Escala Valorativa	Escala Cuantitativa	Descripción
MB: Muy Bajo		1	0 a 500.000
B: Bajo		2	501.000 a 1.500.000
M: Medio		3	1.501.000 a 3.000.000
A: Alto		4	3.001.000 a 5. 000.000
MA: Muy alto		5	5.001.000 o más

Fuente. MAGERIT- Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

9.2.2. Análisis de vulnerabilidades.

Este análisis se realiza con el fin de identificar las amenazas existentes dentro y fuera de la compañía, que afectan la seguridad de la información tanto de los clientes como de la empresa, afectando la continuidad del negocio, los servicios suministrados a los clientes y la información de los mismos.

En este análisis se deben contemplar los puntos de acceso y puertos abiertos desde los cuales se puede acceder remotamente; también se deben identificar las redes inalámbricas existentes dentro y fuera de la compañía, posibles fallas de códigos de página.

Para el análisis se realiza una matriz de vulnerabilidades, amenazas y riesgos la cual se completa realizando observación en campo y hacking ético. A continuación se explican las herramientas mediante las cuales realiza el análisis de vulnerabilidades:

9.2.2.1. Identificación de acceso y puertos abiertos

La identificación del acceso y puertos web se realiza mediante la distribución Linux Kali, la cual contiene herramientas para el análisis de redes mediante hacking ético y así determinar posibles accesos que podrían ser utilizados por personal ajeno a la compañía.

9.2.2.2. Verificación de redes inalámbricas y accesos web.

La verificación se realiza mediante el software libre Acrylic Wi-fi Professional el cual permite identificar las redes inalámbricas que detecta un equipo con tarjeta de red y las características de dicha red, en este caso la red de la compañía. Teniendo en cuenta el protocolo IEEE 802.11. También se identifican la configuración de seguridad del router que soporta a los equipos de la compañía el servicio de internet.

9.2.3. Identificación de requerimientos de seguridad para la compañía.

De acuerdo al análisis de vulnerabilidades efectuado se determinaran los requerimientos de seguridad necesarios para proteger los activos que se encuentren inseguros y accesibles a ataques de software y hardware por personal ajeno a la compañía Indaire Ingeniería S.A.S. Estos requerimientos de seguridad se establecen de acuerdo a la norma ISO/IEC 27001:2003.

Para la identificación de requerimientos de seguridad se debe tener en cuenta que la compañía requiere seguridad física y seguridad virtual. A continuación se explican cada uno de los servicios:

9.2.3.1. Servicios de protección físicos.

El hardware es el elemento del cual depende principalmente la compañía y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización. Los problemas que se pueden afrontar son bastantes, debido a esto se deben tomar las medidas correspondientes para evitarlos. En primera medida debemos analizar la seguridad física ya que si alguien tiene acceso a los servicios de manera física el resto de las medidas son inútiles ya que el sistema falla completamente.

Muchos ataques son triviales, como por ejemplo los de denegación de servicio; si se apaga una máquina que proporciona un servicio es evidente que nadie podrá acceder a esta.

Otro tipo de ataque físico se simplifica en el robo físico, es decir, sustraer los discos duros en los cuales se encuentra la información vital de la compañía y el usuario en cuestión.

Para evitar todo este tipo de inconvenientes deberemos establecer mecanismos de prevención (control de acceso) y de detección, si uno de estos mecanismos falla debemos proveer un sistema básico el cual nos indique que se creó una brecha de seguridad. La identificación exacta de los servicios de protección física se evidencia en la fase de desarrollo.

9.2.3.2. *Servicios de protección virtuales*.

De igual modo que con los servicios físicos se tienen en cuenta los activos y los requerimientos de la compañía pero en este caso los servicios van enfocados

hacia la protección de los bienes virtuales de la compañía. También se realiza una tabla donde se especifica el elemento, su función y el activo virtual que protege.

En la protección de los datos es importante señalar que su manejo y almacenaje está basada en la tecnología la cual permite la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesamiento. Es considerable el acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información. Pero esto igualmente presenta un riesgo considerable ya que al ser digital la información es posible una infiltración en los sistemas y podría ser sustraída de los servidores y ser utilizada para fines lucrativos, esto afecta su disponibilidad y la pone en un alto riesgo. La identificación exacta de los servicios de protección virtual se evidencia en la fase de desarrollo.

9.2.4. Costos de implementación del sgsi en la empresa Indaire ingeniería s.a.s.

Teniendo en cuenta la norma ISO/IEC 27001 y la actividad económica de la empresa se inicia con la identificación del costo de la implementación de cada una de las fases del sistema.

Los costos que se ven reflejados en la implementación del sistema incluyen campañas de concientización del personal, implementación, certificación y mantenimiento del sistema.

9.2.4.1. Cotización de equipos y servicios físicos y virtuales.

En primera medida en el sistema se debe realizar la cotización de los elementos físicos y virtuales que son requeridos para elevar el nivel de seguridad. La cotización se diseña en dos fases las cuales contemplan la fase de implementación y la fase de mantenimiento del sistema, estas se deben cotizar según el nivel de seguridad que más se acomoda a las necesidades de la compañía de acuerdo a su actividad económica.

9.2.4.2. Cotización de implementación del SGSI.

De acuerdo a las cotizaciones previas realizadas y a las necesidades encontradas de seguridad y protección dentro de la compañía se realiza un cuadro en el cual se especifica los costos asociados a cada una de las fases de implementación del

SGSI en la empresa y la certificación del mismo. Este cuadro mencionado se encuentra en la etapa de desarrollo del presente proyecto.

9.2.4.3. Cotización del mantenimiento del sistema

Cuando ya se tiene cotizado el sistema en general para la compañía se realiza una cotización adicional que contemple el mantenimiento continuo del sistema de gestión de la seguridad informática en la empresa para que así el sistema sea eficaz y autosustentable. Esta cotización de igual modo se encuentra en la etapa de desarrollo del proyecto.

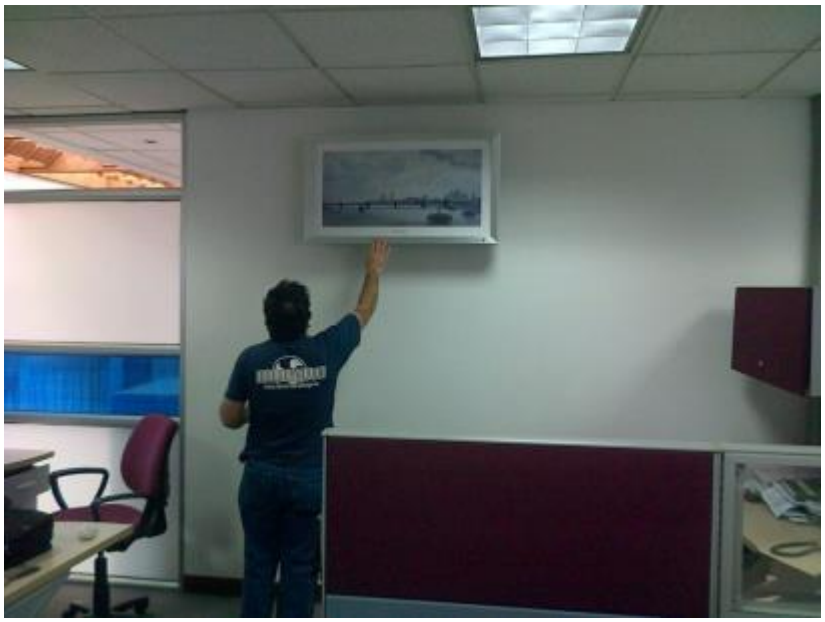
10. DESARROLLO DEL PROYECTO

10.1. IDENTIFICACIÓN DE LOS ACTIVOS DE LA EMPRESA.

Para la identificación de activos se realiza una visita de reconocimiento en la que se recopila información de cada activo mediante una matriz de identificación y registros fotográficos.

Se identifica que la empresa cuenta con nueve activos informáticos importantes que intervienen en el proceso. A continuación en las figuras de la 5 hasta la 9 se evidencia el registro fotográfico realizado en la visita de inspección.

Figura 5. Fotografía de la oficina Indaire Ingeniería s.a.s.



Fuente. Propia.

Figura 6. Sistemas de aire acondicionado.

Fuente. Propia.

Figura 7. Equipos y personal de oficina.

Fuente. Propia.

Figura 8. Tablero de Control

Fuente. Propia.

Figura 9. Componentes del aire acondicionado.

Fuente. Propia.

En la Figuras 6 y 9 se identifican los sistemas y componentes del aire acondicionado, los que son fuente económica principal de la compañía, razón por la que la información de planos y demás de estos productos se clasifica como información prioritaria para la compañía. En la figura 8 se observa el tablero de control eléctrico de las instalaciones de la compañía.

A continuación en la tabla 6 se muestra la matriz de identificación de activos tecnológicos, en la que se realiza la valoración cualitativa y cuantitativa de los mismos.

Tabla 6. Matriz de identificación de activos tecnológicos.

Nombre del Documento:	Matriz de activos de información		
Nivel de Confidencialidad:	**Confidencial:** No debe ser conocido por personal ajeno al proceso de Gestión de Seguridad de la Información. No puede ser distribuido públicamente.		
Codificación:	R-GSI-001	**Versión:**	1.0
Fecha de última modificación:	19/10/2015	**Fecha de Creación:**	19/10/2015
Responsable del documento:	Oscar Javier Zaque González		
Aprobado por:	INDAIRE INGENIERIA		

Fecha Visita	Nombre del Activo	Tipo de Activo	Software	Función	Descripción del Activo	Característica Hardware	Valoración Cualitativa	Valoración Cuantitativa	Valoración Final	Imágenes
16-oct	Computador de Escritorio	Aplicaciones	Auto CAD, office	Elaboración de planos y diseños	Diseños elaborados específicamente para clientes según necesidades por procesos internos del cliente.	Memoria RAM 4Gb Disco Duro 750 Gb Procesador Core I-3 Tarjeta de Video G-Force 8400	Alto	Bajo	Medio	
16-oct	Computador de Escritorio	Datos / información	Windows, office	Elaboración de cotización y certificados	Cotizaciones elaboradas para clientes donde especifica de la distribución interna de la compañía que requiere el servicio.	Memoria RAM 4Gb Disco Duro 500 Gb Procesador Core 2 Dúo 3,0 Tarjeta de Video Ati Radeon 9500	Alto	Bajo	Medio	

Tabla 6. (Continuación).

Fecha Visita	Nombre del Activo	Tipo de Activo	Software	Función	Descripción del Activo	Característica Hardware	Valoración Cualitativa	Valoración Cuantitativa	Valoración Final	Imágenes
16-oct	Computador de Escritorio	Datos / información	World office, office	Elaboración de cuentas y nomina	Costos analizados según los requerimientos del cliente, costos de gastos de nómina.	Memoria RAM 4Gb Disco Duro 500 Gb Procesador Core 2 Dúo 3,0 Tarjeta de Video Ati Radeon 9500	Alto	Bajo	Medio	
16-oct	Computador de Escritorio	Aplicaciones	Windows, Auto CAD	Elaboración de planos superficiales, trabajo de campo.	Elaboración de planos eléctricos y físicos de los montajes realizados.	Memoria RAM 4Gb Disco Duro 1Tb Procesador Core I-7 Tarjeta de Video Ati Radeon 9500	Alto	Bajo	Medio	
16-oct	Computador Portátil	Activo físico informático	Windows, office	Elaboración de planes de mantenimiento preventivo	Rutinas definidas para cada uno de los clientes de acuerdo del sistema implementado.	Memoria RAM 4Gb Disco Duro 500Gb Procesador Core I-5	Alto	Medio	Alto	
16-oct	Computador de Escritorio	Activo físico informático	Windows, office	Búsqueda de posibles clientes y venta de equipos.	Base de datos de los clientes y los costos de importación de equipos.	Memoria RAM 2Gb Disco Duro 320Gb Procesador Core 2 Dúo	Alto	Bajo	Medio	

Tabla 6. (Continuación).

Fecha Visita	Nombre del Activo	Tipo de Activo	Software	Función	Descripción del Activo	Característica Hardware	Valoración Cualitativa	Valoración Cuantitativa	Valoración Final	Imágenes
16-oct	Computador de Escritorio	Activo físico informático	Windows, office	Realización de proceso de montajes y puesta en marcha	Rutinas de mantenimiento, informes de instalación, mediciones iniciales e información de montajes en cada uno de los clientes.	Memoria RAM 2Gb Disco Duro 320Gb Procesador Core 2 Dúo	Alto	Bajo	Medio	
16-oct	Impresora Laser	Equipos Informáticos	N.A	Impresión de formatos, cuentas de cobro y recepción de fax	Conexión telefónica para la recepción de fax. Cuenta con conexión alámbrica desde los computadores.	Impresora Láser Hp	Muy Bajo	Medio	Bajo	
16-oct	Teléfono fijo	Redes de Comunicaciones	N.A	Recepción y envío de llamadas telefónicas.	Conexión telefónica para la recepción y envío de llamadas.		Muy Bajo	Muy Bajo	Muy Bajo	
16-oct	Camioneta	Activo Físico Móvil	N.A	Transporte de equipos, visita a clientes, compra de materiales.	N.A	N.A	Muy Bajo	Muy Alto	Medio	

Tabla 6. (Continuación).

Fecha Visita	Nombre del Activo	Tipo de Activo	Software	Función	Descripción del Activo	Característica Hardware	Valoración Cualitativa	Valoración Cuantitativa	Valoración Final	Imágenes
16-oct										
	Contador	Personal	N.A	Se encarga de la administración de activos físicos e intangibles.	Encargado de la administración de activos físicos e intangibles de la Empresa, nóminas y pagos.	N.A	Medio	Medio	Medio	
16-oct	Diseñador	Personal	N.A	Se encarga de realizar los diseños geométricos y estructurales del sistema de aire acondicionado.	Los diseños que realiza dependen de lo que exige el cliente y de la norma técnica que se deba implementar para dichos diseños.	N.A	Medio	Medio	Medio	
16-oct	Administradora	Personal	N.A	Se encarga de la incorporación del personal.	Define nóminas y temas relacionados con Salud Ocupacional.	N.A	Medio	Medio	Medio	
16-oct	Gerente General	Personal	N.A	Se encarga de supervisar al área de diseño como al área de instalación y mantenimiento.	También es el encargado de las relaciones comerciales de la compañía.	N.A	Medio	Alto	Alto	

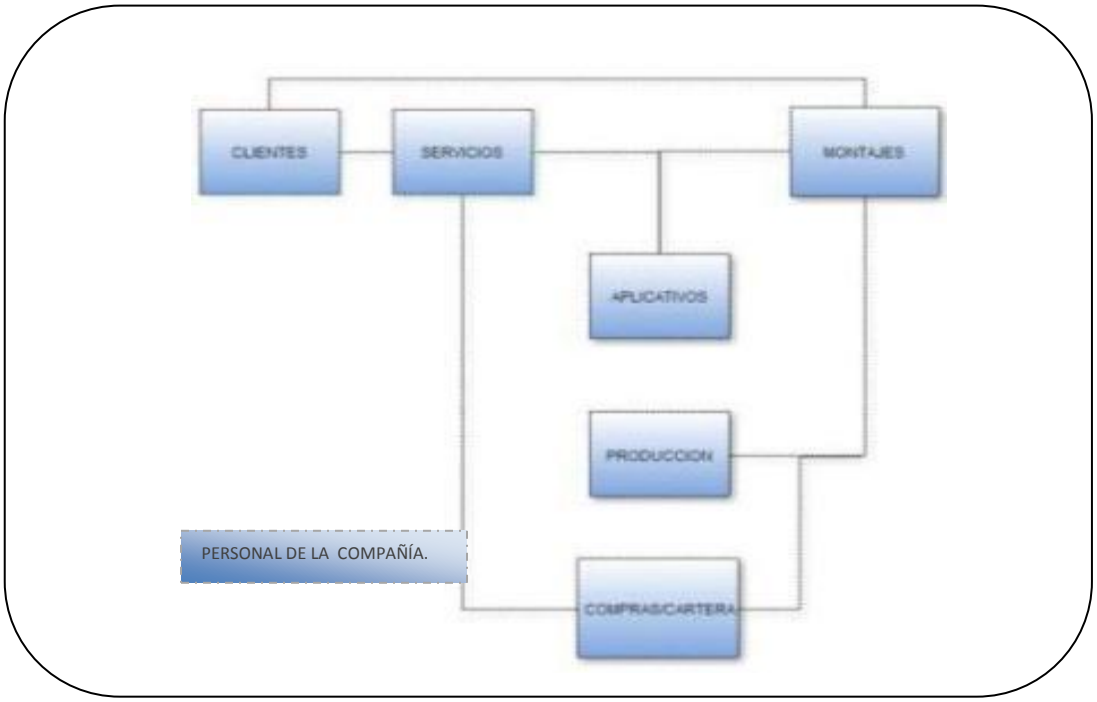
Fuente. Autor.

La clasificación e identificación de los activos se realiza teniendo en cuenta el estado del activo tecnológico, el tipo de activo y sus características en software y hardware en caso de ser físico tecnológico. La matriz que se realizó permite conocer con exactitud los activos tecnológicos a los que se les va a hacer el estudio de vulnerabilidades y amenazas. La escala de valoración tanto cualitativa como cuantitativa se explica en el numeral 9.1.1 en el diseño metodológico.

10.1.1. Dependencia entre Activos.

En el siguiente esquema se identifica el árbol dependencia entre los activos tecnológicos de la compañía Indaire Ingeniería s.a.s., de acuerdo a la interacción de la información entre ellas.

Figura 10. Árbol de dependencia entre Activos.



Fuente. Autor.

10.2. ANÁLISIS DE VULNERABILIDADES.

El análisis de vulnerabilidades se realiza teniendo en cuenta la matriz de identificación de activos realizada con base a la información obtenida en la empresa.

Se inicia con la identificación de cada IP usando las herramientas de administración que ofrece el sistema operativo Windows. Primero se accede al comando cmd. Cuando ya se encuentra abierta la herramienta de comandos de Windows se digita e ingresa al comando ipconfig, este comando entrega información de la IP asociada al equipo y otras descripciones. Esto se realiza con el fin de excluir a modo de prueba error cada IP que es utilizada por equipos contenidos en la red e identificar las IP que se encuentran en la red pero por equipos que no se encuentran autorizados. A continuación se presenta la tabla 7 en la que se muestran las IP encontradas en la red.

Tabla 7. IP Encontradas en la red.

ACTIVO	IP
Computador 1	192.168.1.101
Computador 2	192.168.1.100
Computador 3	192.168.1.105
Computador 4	192.168.1.106
Computador Portátil 5	192.168.1.117
Computador 6	192.168.1.113

Fuente. Autor

Se identifica que las IP encontradas en la red se encuentran asociadas a los equipos de la compañía, es decir no se encuentra alguna IP intrusa en la red.

10.2.1. Identificación de acceso y puertos abiertos

Cuando ya se conocen las IP de cada computador o dispositivo que se encuentra en la red se procede a realizar la identificación de la red mediante la herramienta Nmap del software Kali Linux. En la siguiente figura (Figura 11) se muestra el escaneo a la red realizado por medio de la herramienta.

Figura 11. Identificación de dispositivos conectados a la red.

Fuente. Kali Linux

En la identificación se encuentran seis IP, las cuales corresponden a los equipos de la red local de la compañía.

Una vez realizada la identificación de los dispositivos conectados a la red se continúa con la verificación de los puertos que se encuentran abiertos en cada una de las unidades mediante un escaneo por medio de la herramienta Nmap de Kali Linux.

Los datos obtenidos del escaneo de cada IP en el software se presentan en la tabla 8. En el anexo número 2 se muestran los pantallazos de los escaneos.

Tabla 8. Identificación de puertos abiertos.

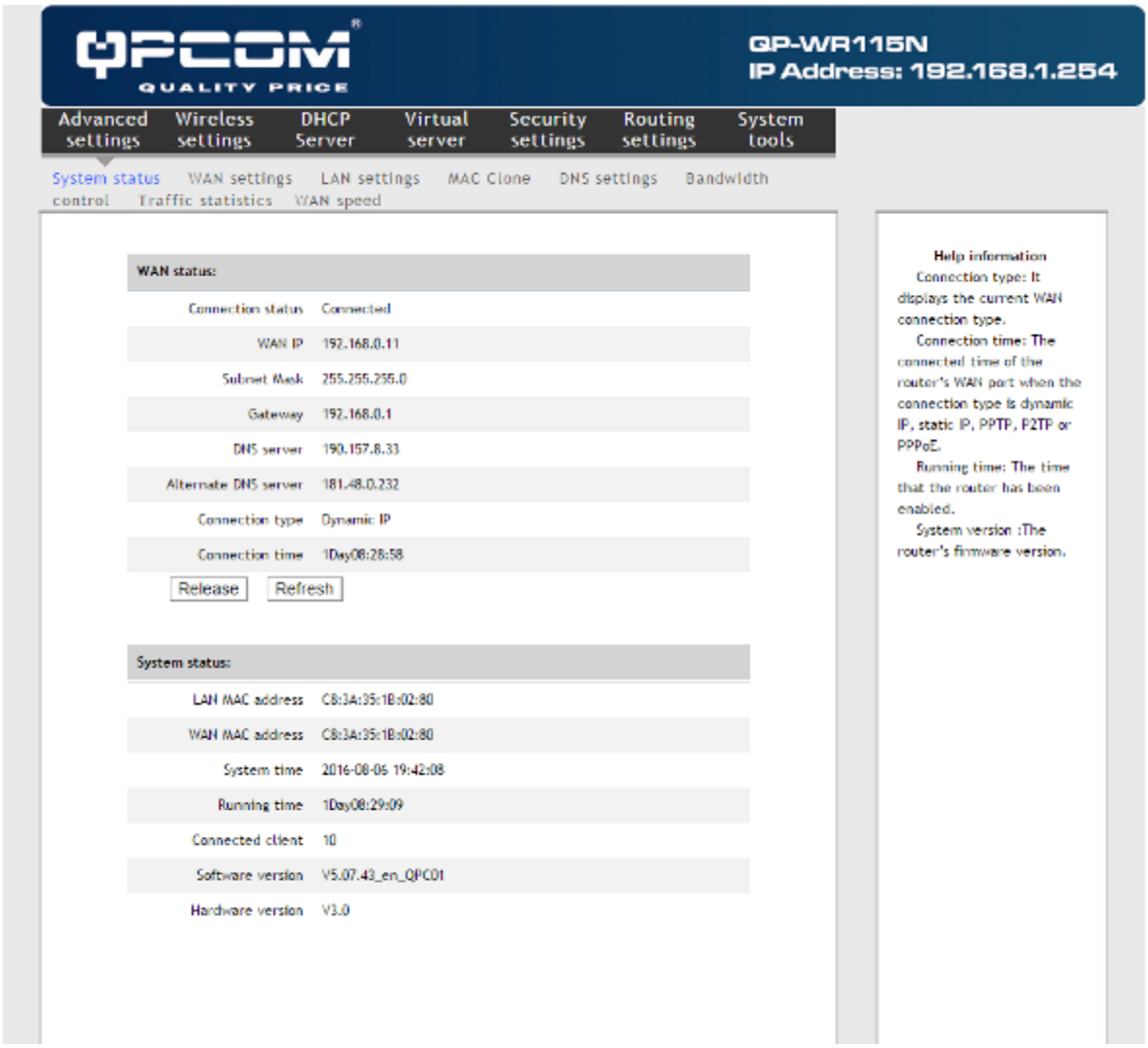
Activo	IP	No. de Puertos Abiertos
Computador 1	192.168.1.101	6
Computador 2	192.168.1.100	5
Computador 3	192.168.1.105	7
Computador 4	192.168.1.106	10
Computador Portátil 5	192.168.1.117	7
Computador 6	192.168.1.113	0

Fuente. Autor

10.2.2. Verificación de redes inalámbricas y accesos web.

Se identifica una red inalámbrica de internet en la compañía que se encuentra ubicada en un punto estratégico para soportar a todos los equipos del servicio de internet. Para identificar las características de la red inalámbrica se procede a verificar la configuración del router. En las figuras 12 y 13 se muestran la configuración del router y la configuración de la red LAN.

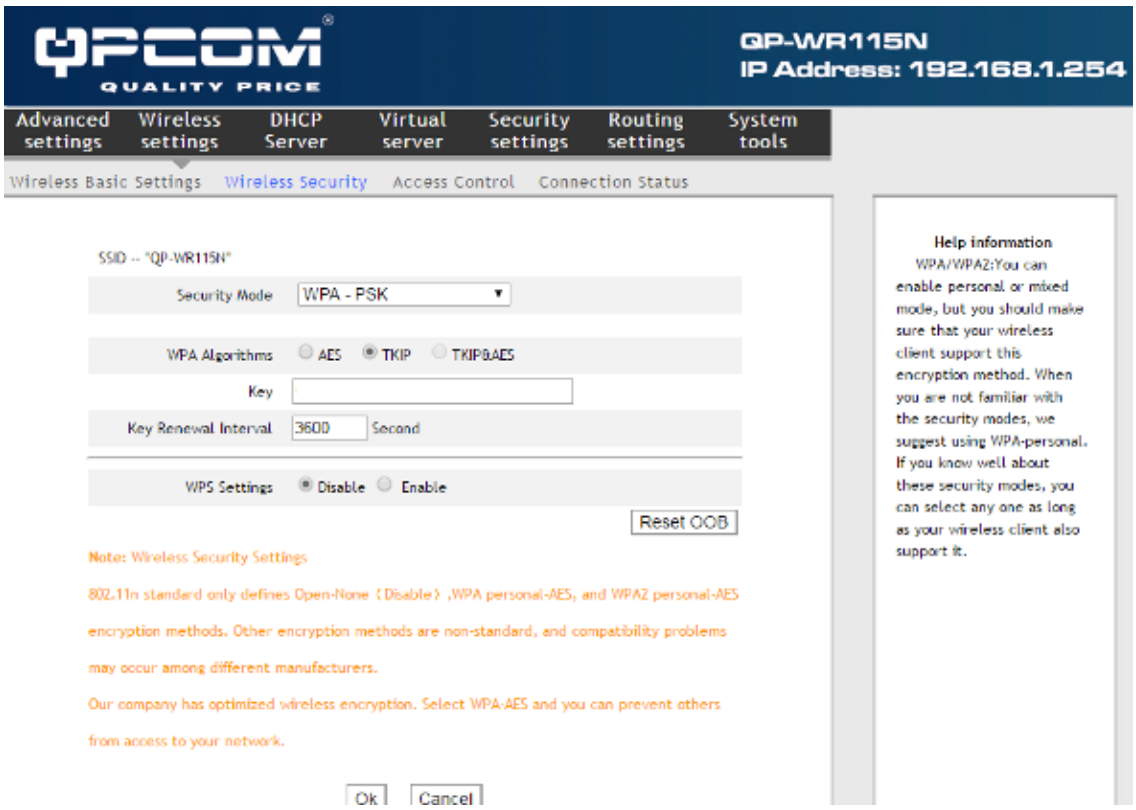
Figura 12. Configuración de la red LAN.



Fuente. QPCOM. Inc.

En la figura 12. Se identifica que el tipo de conexión es dinámica, así mismo se puede evidenciar la máscara de sub-red, entre otras características de la red Wifi.

Figura 13. Configuración del router.



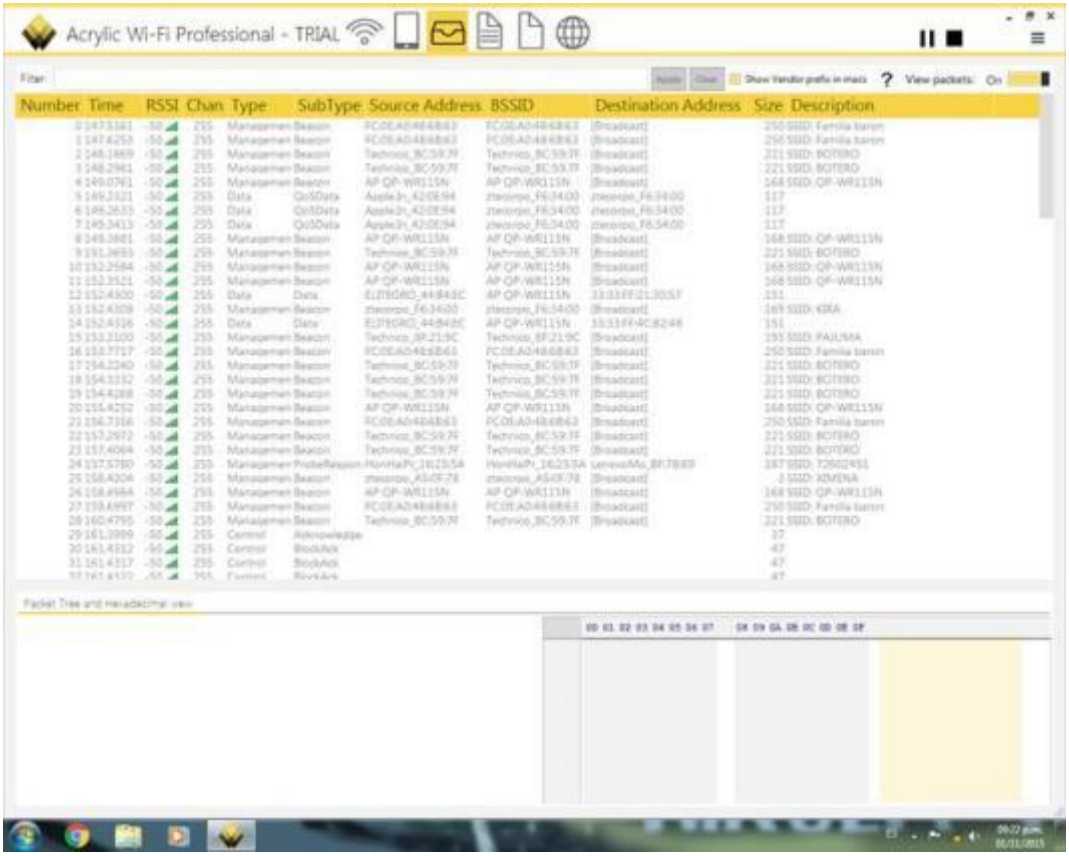
Fuente. QPCOM. Inc.

La información que provee la imagen incluye el tipo de seguridad que se encuentra activa así como la contraseña utilizada para el acceso a la red inalámbrica. En este caso la configuración WPS se encuentra deshabilitada.

Ya identificadas las características del router se procede con el análisis de la red Wi-fi mediante el software libre Acrylic Wi-fi. Este software compatible la plataforma Microsoft Windows permite identificar las vulnerabilidades de seguridad existentes en las redes Wi-fi que se encuentren al alcance de la tarjeta de red del equipo. También recopila información relacionada con canales de emisión e intensidad.

En la figura 14 se muestra la plataforma del software Acrylic Wi-fi y la búsqueda de redes Wi-fi que detecta la tarjeta de red del equipo.

Figura 14. Análisis con Acrylic Wifi

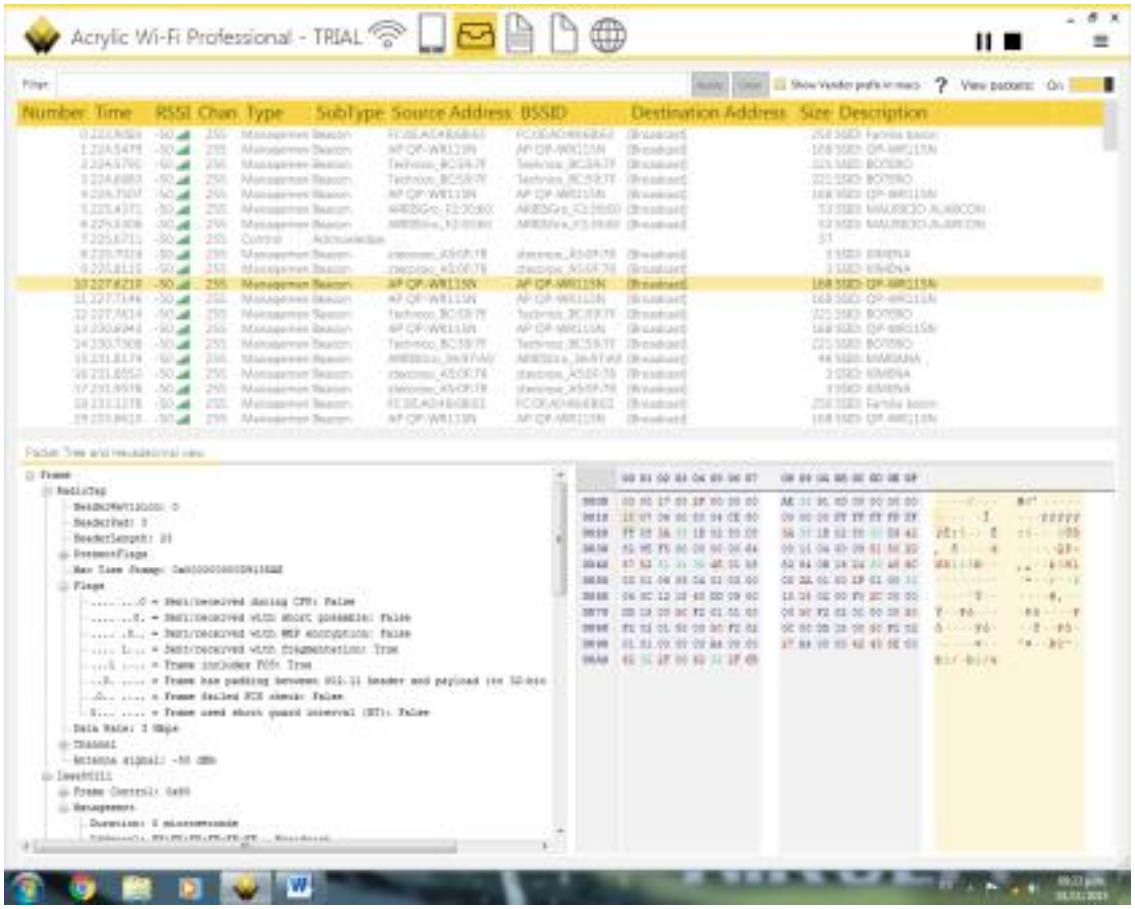


Fuente. Acrylic Wi-Fi Professional

Luego de identificar las redes Wi-fi que detecta la tarjeta de red, se busca la red que se desea analizar en este caso la red AP QP-WR115N que es la red de la compañía Indaire Ingeniería s.a.s. Luego de encontrarla en el listado aportado por el software, se selecciona la red y el software en la parte inferior de la plataforma muestra las características internas de la red wi-fi. Al encontrar las características internas de la red, esta se encuentra vulnerable a ataques o infiltraciones.

En la figura 15 se evidencian las características internas de la red Wi-fi de Indaire Ingeniería aportadas por el software Acrylic Wi-Fi Professional.

Figura 15. Características internas de la red Wi-fi de Indaire Ingeniería s.a.s.



Fuente. Acrylic Wi-Fi Professional

En la imagen 15 se identifican algunas características de la red, co: Dirección Mac, bssid, tipo de conexión, así como la descripción específica de los frame enviados y recibidos.

10.2.3. Análisis de vulnerabilidades físicas a activos tecnológicos.

En la visita de campo que se realiza para la identificación de cada activo, también se identifica el estado físico en el que se encuentra el activo y se valora de acuerdo a la siguiente escala:

Tabla 9. Escala de Valoración de Vulnerabilidades físicos a activos tecnológicos

Escala de Valoración	Descripción
Buen Estado	Activo en buen estado físico y excelente funcionamiento
Estado Regular	Activo en funcionamiento pero estado físico regular
Mal Estado	Activo en mal estado físico y sin funcionar

Fuente. Autor

A continuación se muestra la tabla 10 en la cual se identifican las vulnerabilidades de los activos tecnológicos según su condición física, escalas de valoración cualitativa y cuantitativa teniendo en cuenta el numeral 8.2.1.1 del presente proyecto.

Tabla 10. Análisis de Vulnerabilidades físicas de activos tecnológicos.

Tipo de Activo	Nombre del Activo	Estado Físico	Valoración Cualitativa	Valoración Cuantitativa	Descripción
Aplicaciones	Computador de Escritorio	En buen estado	4	3	
Datos / información	Computador de Escritorio	En buen estado	5	3	
Datos / información	Computador de Escritorio	En buen estado	5	3	
Aplicaciones	Computador de Escritorio	Mal Estado	4	3	Requiere Cambio de la batería para su correcto funcionamiento
Activo físico informático	Computador Portátil	En buen estado	5	3	
Activo físico informático	Computador de Escritorio	En buen estado	5	3	
Activo físico informático	Computador de Escritorio	En buen estado	5	3	
Equipos Informáticos	Impresora Laser	En buen estado	3	2	
Redes de Comunicaciones	Teléfono fijo	Estado Regular	2	1	Requiere Cambio del cable entre la bocina y el tablero para su correcto funcionamiento

Fuente. Autor.

10.2.4. Matriz de vulnerabilidades.

Ya finalizado la identificación de vulnerabilidades tanto físicas como de infiltración de software y red se procede a realizar la matriz de vulnerabilidades, amenazas y riesgos. La matriz permite conocer el nivel de seguridad de activos tecnológicos y redes con el que cuenta la empresa. En la tabla 11 se identifica el riesgo dependiendo de las amenazas y vulnerabilidades.

Tabla 11. Identificación del Riesgo.

Tipo de Activo	Amenaza	Vulnerabilidad	Riesgo	Activos que interviene	Probabilidad de Ocurrencia					Impacto					Valoración Final
					1	2	3	4	5	1	2	3	4	5	
Software	Falta de seguridad en el sistema.	Ataque a Software	Medio	Computadores			3							5	4
	Backup inseguro	Perdida de Información	Alto	Computadores			3							5	4
	Software Desactualizado	Virus	Alto	Computadores				4						5	5
	Acceso con clave ajena	Acceso a información sensible	Medio	Computadores			3						4		4
	Extracción de información	Falla de bloqueo de puertos usb/cd	Alto	Computadores				4						5	5
	Uso inadecuado de Internet	Acceso a páginas web prohibidas	Alto	Computadores					5				4		5
Hardware	Falta de seguridad física e infraestructura	Acceso de personas no autorizadas	Medio	Computadores		2						3			3
	Accidente con líquidos	Manipulación inadecuada de líquidos/alimentos	Medio	Computadores			3							5	4

Tabla 12. (Continuación).

Tipo de Activo	Amenaza	Vulnerabilidad	Riesgo	Activos que interviene	Probabilidad de Ocurrencia					Impacto					Valoración Final
					1	2	3	4	5	1	2	3	4	5	
	Falta de equipos de regulación de voltaje	Fallas eléctricas	Medio	Computadores, impresoras, teléfonos				4						5	5
	Uso inadecuado de activos tecnológicos	Deterioro de activos	Medio	Computadores, impresora, teléfonos			3					3			3
	Falta de Firewall	Acceso a la información	Alto	Computadores, impresora, teléfonos					5					5	5
	falla en el servidor/ Almacenamiento	falla física en el disco, robo del mismo	Alto	Computadores			3							5	4
	Falta de mantenimiento de equipos	Fallas por suciedad	bajo	Computadores, impresora, teléfonos		2					2				2
Comunicaciones	Inadecuada transmisión de la información	Snirfing	Medio	Información y datos		2							4		3
	Red de comunicación abierta	Escucha de información por terceros	Medio	Teléfonos / Wifi		2						3			3
	Interferencia electromagnética/eléctrica	Comunicación deficiente	Medio	Teléfonos/Fax		2						3			3
Seguridad Física	Falta de control de acceso de personal no autorizado	Robo de hardware, software o datos.	Alto	Computadores, impresora, teléfonos, datos				4						5	5

Tabla 13. (Continuación).

Tipo de Activo	Amenaza	Vulnerabilidad	Riesgo	Activos que interviene	Probabilidad de Ocurrencia					Impacto					Valoración Final
					1	2	3	4	5	1	2	3	4	5	
	Bajos niveles de protección de instalaciones físicas	Robo de hardware, software o datos.	Alto	Computadores, impresora, teléfonos, datos				4						5	5
Personal	Falta de capacitación	errores de implementación de políticas	Alto	Computadores, impresora, teléfonos, datos			3							5	4

En la tabla 12 se evidencia la matriz de Vulnerabilidades, amenazas y riesgos de Indaire Ingeniería s.a.s.

Tabla 14. Matriz de Riesgos.

PROBABILIDAD		ACTIVO				
		ESTRUCTURA	SEG. FISICA	SOFTWARE	HARDWARE	INFORMACION
RIESGO	ATAQUES/VIRUS					
	PROVEEDORES					
	USO INDEBIDO					
	ROBO					
	NATURALES					

Nivel	Impacto
	Bajo
	Medio
	Alto

Fuente. CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.28.

Se identifica que la compañía Indaire Ingeniería requiere un SGSI ya que se encuentra en riesgo de sufrir ataques a sus activos tanto físicos como tecnológicos.

10.3. IDENTIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD PARA LA COMPAÑÍA.

Teniendo en cuenta el análisis de vulnerabilidades se procede a determinar los requerimientos de seguridad necesarios para proteger los activos y la información contenida en ellos que se encuentren inseguros y accesibles a ataques de software y hardware por personal ajeno a la compañía Indaire Ingeniería S.A.S.

Se toma la norma técnica ISO/IEC 27001:2013. Como base para identificar qué tipo de requerimientos de seguridad necesita la compañía y se establecen los siguientes puntos a tener en cuenta para la correcta implementación de la norma.

10.3.1. Obtener el Apoyo de la Dirección.

Según la ISO 27001 como primera medida para poder realizar la implementación de un SGSI en la compañía, la gerencia de la misma debe dar su aval y apoyo logístico y económico. También es importante que la gerencia tome la implementación del SGSI como un proyecto para que así su implementación sea eficaz e involucre a todo el personal de la compañía.

10.3.2. Definición de alcance.

Definir el alcance del SGSI para la compañía es un paso fundamental para el desarrollo del sistema ya que a través de este se establecerán los pasos a seguir para la elaboración e implementación del sistema de seguridad para la empresa.

Para la definición del alcance, elaboración e implementación del SGSI se requiere un asesor interno capacitado en los sistemas de gestión de la seguridad informática.

Se proyecta que el tiempo estimado para que el asesor interno en conjunto con la dirección de la compañía para la redacción del alcance sea de 30 días hábiles.

10.3.3. Redacción de las políticas de seguridad.

La redacción de las políticas de seguridad es fundamental para la definición de normas del uso correcto de los sistemas de información en la compañía para todos los usuarios y personal en la misma.

La política de seguridad la define el asesor interno que trabaja en el SGSI en la empresa y la establece teniendo en cuenta los procesos y necesidades de la compañía. De igual forma que con el alcance del SGSI se determina que el asesor interno debe redactar las políticas de seguridad en un tiempo estimado de 30 días calendario.

10.3.4. Definición de la Metodología de evaluación de riesgos, Evaluación de riesgos y tratamiento de riesgos.

Como lo dice (Dejan Kosutic, 2010) "*La evaluación de riesgos es la tarea más compleja del proyecto para la norma ISO 27001; su objetivo es definir las reglas para identificar los activos, las vulnerabilidades, las amenazas,*

las consecuencias y las probabilidades, como también definir el nivel aceptable de riesgo." De la definición correcta de metodología para la evaluación de riesgos depende el correcto tratamiento de los mismos. Esta metodología de evaluación de riesgos la define el asesor interno.
Luego de conocer la metodología exacta para la evaluación de riesgos se procede a evaluar los mismos, en este proyecto de grado se realizó la evaluación de riesgos para la compañía y por lo tanto se tienen recomendaciones de protección física para la misma

Los requerimientos de seguridad físicos identificados durante el análisis de activos, riesgos, vulnerabilidades y amenazas, se plasman en la tabla número 13.

Tabla 15. Recomendaciones de protección para la compañía.

Elemento	Descripción
Firewall Físico	Debido a la cantidad de ataques presentes a los medios informáticos de la industria se hace necesaria la implementación de un sistema de protección, el cual impida la interceptación del tráfico de datos sensibles de la compañía.
CCTV	El circuito cerrado de televisión asegura las áreas vulnerables con un sistema de video el cual se encuentra monitoreado por el personal a cargo para así detectar cualquier irregularidad dentro de las instalaciones de la compañía.
Antivirus	La instalación de un sistema de antivirus con licencias originales ayuda a mejorar considerablemente la seguridad de la red ya que cuenta con las actualizaciones y servicios adicionales que ofrecen, tales como exclusiones y soporte en caso de falla del producto. Cobertura para 10 equipos.
Endpoint	Un módulo adicional del sistema Kaspersky ayuda a mejorar las brechas de seguridad existentes ya que es un módulo especializado para empresas así como para los servidores de varias plataformas. Ofrece controles de aplicaciones y dispositivos.
Control de acceso	El control de acceso esta soportado por un sistema de control biométrico en el cual se puede estipular el personal que puede ingresar al área, en este caso se hace referencia a los ingenieros que manejan la plataforma así como los medios de almacenamiento de la compañía.
Detectores de humo	En caso de la existencia de material en combustión la reacción química activa los detectores de humo logrando activar los sistemas contra incendio de las instalaciones. Aunque este tipo de sistemas puede llegar a afectar los equipos electrónicos minimiza el daño que podría causar el fuego.

Tabla 13. (Continuación).

Elemento	Descripción
Extintores	El área a cubrir es relativamente pequeña por lo que el costo de implementación de un sistema de extinción de incendios es bastante alto y no justifica la inversión por lo cual se opta por implementar extintores manuales de polvo químico seco. 4 Unidades.
UPS	El flujo eléctrico constante en la compañía es vital para el buen funcionamiento de los equipos por lo cual se recomienda la implementación de un sistema de regulación y soporte "UPS" el cual soporta la red en caso de un corte de energía o una sobrecarga en la red. Se sugiere una ups de 3KVA lo cual es suficiente para soportar la cantidad de equipos conectados a la red por 30 minutos aproximadamente.
Polo a tierra	El polo a tierra se compone de una varilla Cooper Well de 1,8 mts la cual se instala en el piso para asegurar cualquier tipo de descarga a tierra. Esto protege a la infraestructura completa de la compañía. El costo asociado incluye la instalación de la misma.

Fuente: Autor

10.3.5. Redacción de la Declaración de Aplicabilidad y el plan de tratamientos.

Luego de realizar la definición de los riesgos y el tratamiento de los mismos se inicia con la redacción de la declaración de aplicabilidad la cual define los controles a realizar y define cuales de esos controles son aplicables. La redacción del plan de tratamiento define las directrices de implementación de los controles y tratamientos para los riesgos en la empresa.

La redacción de estos documentos la realiza el asesor interno que trabaja con la compañía.

10.3.6. Implementación de Programas de Capacitación y Concientización.

Hace parte de la ejecución del SGSI la implementación de programas de capacitación y sensibilización, estos programas van enfocados al personal de la compañía con el fin de brindarles inducción sobre las temáticas del SGSI y crear buenas prácticas de manejo de la información. Los programas de capacitación y concientización son supervisados por el asesor interno pero implementado por un capacitador.

10.3.7. Puesta en Marcha del SGSI.

Cuando ya se tenga el sistema diseñado se procede a iniciar la fase de puesta en marcha del sistema, de cada procedimiento se debe tener registro. Esta fase del SGSI la controla el asesor interno.

10.3.8. Supervisión del SGSI por medio de Auditoría Interna Periódica.

Se realiza simultáneamente a la fase de puesta en marcha del SGSI, se identifica si el sistema funciona correctamente y en caso de no ser así se implementan acciones correctivas de acuerdo a los hallazgos observados. Las auditorías internas la realiza el asesor interno.

10.3.9. Revisión por parte de la dirección.

Se realiza la entrega del informe general del avance del sistema y así como el informe de fallas y acciones correctivas. La gerencia debe estar debidamente informada sobre todo lo relacionado con el SGSI.

10.3.10. Certificación Icontec

El propósito principal de la implementación del SGSI es proteger la compañía de posibles ataques a la información y activos de la empresa, adicional a esto se busca certificar el sistema ante el Icontec. Al obtener la certificación se identifica que el sistema funciona correctamente.

10.4. COSTOS DE IMPLEMENTACIÓN DEL SGSI EN LA EMPRESA INDAIRE INGENIERÍA S.A.S.

Los costos de implementación del sistema de gestión de la seguridad de la información se realizan teniendo en cuenta los requerimientos del SGSI para la compañía ya identificados y descritos en el anterior numeral.

Se toma cada uno de los requerimientos del sistema como una fase independiente, posteriormente se identifican los recursos necesarios para completar cada una de las fases y se realizan cotizaciones de cada recurso para así definir los costos de implementación de cada una de las fases y posterior a esto del sistema en general.

En la tabla 12 se evidencia la proyección financiera total del sistema encontrado en el anexo 3.

En el anexo 4 se encuentran las cotizaciones de cada uno de los recursos ya sean humanos o materiales que se recomiendan para llevar a cabo la implementación del sistema.

11. CONCLUSIONES

El sistema de seguridad de información definido para la compañía Indaire ingeniería cubre con los aspectos intrínsecos de su funcionamiento y debe alinearse con actividad de la organización para ser más eficiente en la protección de la información.

El análisis de vulnerabilidades identifica brechas de seguridad, las que pueden permitir intrusiones de personas ajenas a la compañía.

Al usar la escala de riesgo, se logró determinar que el riesgo es Medio Alto, lo cual genera una alerta para la compañía, debido a la ausencia de controles de riesgo interno, por tanto se hace necesaria la implementación de un SGSI.

La utilización de MAREGIT permitió realizar una valoración de vulnerabilidades y asignar una escala de riesgo en la cual se logró determinar que el riesgo es Medio Alto lo cual debe ser de preocupación para la compañía debido a la ausencia de controles de riesgo interno.

La implementación de las políticas de seguridad es fundamental ya que los empleados no tienen un conocimiento base con respecto al manejo y cuidados de la información causa por la cual el riesgo humano aumenta la posibilidad de daño o corrupción de la información interna.

Se recomienda iniciar lo más pronto posible, la creación de un programa de concientización con el fin de empezar a generar una cultura global con enfoque del cuidado de la información, bajo el cumplimiento de políticas claras por la alta gerencia de la compañía.

12. BIBLIOGRAFÍA

CALDERON, Diana y compañía. Implementación de sistema de gestión de seguridad de la información aplicada al área de recursos humanos de la empresa decevale s.a. Guayaquil. 2011. P. 21-25. Escuela de diseño y comunicación visual. Escuela Superior Politécnica del Litoral.

CRUZ ALLENDE, Daniel. Gestión de la Seguridad de la Información. Barcelona. (2006). P. Universidad Abierta de Cataluña – UOC.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 603. (27, Julio, 2000). Por la cual se definen disposiciones sobre los derechos de autor en Colombia y se dictan otras disposiciones. Diario oficial. Bogotá D.C. 2000. No 44.108.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266. (31, Diciembre, 2008). Por la cual se definen disposiciones sobre el habeas data y otras disposiciones. Diario oficial. Bogotá D.C. 2008. No 47.291.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, Enero, 2009). Por la cual se modifica el código penal, se crea la protección a la información como bien jurídico y se dictan otras disposiciones. Diario oficial. Bogotá D.C. 2009. No 47.223.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1527. (27, Abril, 2012). Por la cual se establece el régimen general de la protección de los datos personales y se dictan otras disposiciones. Diario oficial. Bogotá D.C. 2012. No 48.414.

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1377. (27, Julio, 2013). Por el cual se reglamente parcialmente la ley 1581 de 2012, se hacen modificaciones y se dictan otras disposiciones. Diario oficial. Bogotá D.C. 2013. No 48.834.

COMUNIDAD DE MADRID, ÁREA DE ANÁLISIS DE RIESGOS. “Proyecciones Financieras. Plan de formación Comunidad de Madrid”. {En línea}. {13 mayo de 2015}, Disponible en: (http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/proyecciones_financieras_es.pdf.)

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, Procedimientos e Impulso de la Administración Electrónica. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012 pg.27

LANDINO A, Marta. VILLA S, Diana. Fundamentos de Iso 27001 y su aplicación en las empresas. En: Scientia et Technica Año XVII, No 47. Universidad Tecnológica de Pereira. Abril de 2011.

MARQUEZ DE MELO, José “Comunicación e integración latinoamericana: El papel de ALAIC”. {En línea}. {10 julio de 2008} disponible en: (www.mty.itsem.mx/externos/alaic/texto1html).

REVISTA ENTREPRENEUR,” Aprende a hacer proyecciones financieras”. {En línea {13 mayo de 2015}, Disponible en: pp. 1-2. Disponible en: (http://www.soyentrepreneur.com/aprende-a-hacer-proyecciones-financieras.html.)

OFICINA ASESORA DE SISTEMAS UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Proceso de Desarrollo OPEN UP/OAS. Gestión del riesgo. Bogotá. 2012. Capítulo 5 pg. 12.

PATIÑO, Luis Olmedo. Propuesta de actualización y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor. Tesis Especialista en Seguridad Informática. Sanjuán de Pasto. 2014. Pg. 22. Escuela de ciencias Básicas, Tecnología e ingeniería. Universidad Nacional Abierta y a Distancia.

13. ANEXOS

Anexo 1. Carta de aprobación de la compañía.

INDAIRE
Soluciones tecnológicas

Diseño
Instalación
Mantenimiento
Aire Acondicionado
Servicio a Nivel Nacional

Bogotá D.C. Octubre 14 del 2015 CD15-125

Señores
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (PROGRAMA DE ESPECIALIZACIÓN INFORMÁTICA)
Bogotá D.C.

Asunto: Carta de Aceptación Proyecto de Grado en la empresa Indaire Ingeniería S.A.S.

De manera atenta manifestamos nuestro interés y conocimiento de la propuesta de Proyecto de investigación titulada *PROYECCIÓN FINANCIERA Y TECNOLÓGICA REQUERIDA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), BAJO LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA INDAIRE INGENIERÍA S.A.S.*

Elaborada por el estudiante: Oscar Javier Zaque González C.C 80174604

En este sentido, nos comprometemos a participar en este proceso ofreciendo la información y el apoyo necesario para el desarrollo de la propuesta.

Como documento académico conocemos que los resultados del trabajo serán publicados y registrados en la Biblioteca de la UNAD, como elemento de consulta para el público.

Una vez más quedamos a su entera disposición atentos a aclarar cualquier duda que pueda presentársele.

Cordialmente:

CARLOS A. DONOSO
Representante legal

INDAIRE INGENIERIA S.A.S.
BOGOTÁ - COLOMBIA Carrera 26 Nº 52 - 09 sur Teléfono: (1) 602 7262
Celular – 312 4737217 E-mail: *carlos.donoso@indaire.com*

YORK It's time to get comfortable. LG Life's Good SAMSUNG TRANE

Anexo 2. Pantallazos Análisis de Puertos Abiertos de cada IP contenida en la Red, mediante la herramienta Nmap.

Figura 16. Escaneo de puertos 192.168.1.101

Fuente. Kali Linux

Figura 17. Escaneo de puertos IP192.168.1.100

Fuente. Kali Linux

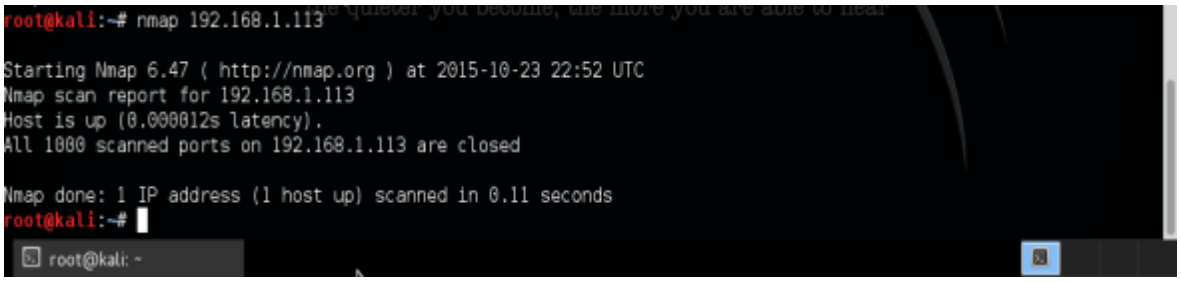
Figura 18. Escaneo de puertos IP192.168.1.105

Fuente. Kali Linux

Figura 19. Escaneo de puertos IP192.168.1.106

Fuente. Kali Linux

Figura 20. Escaneo de puertos IP192.168.1.113



Fuente. Kali Linux.

Figura 21. Escaneo de puertos IP192.168.1.117

Fuente. Kali Linux

Anexo. 3 Proyección Financiera SGSI para la compañía Indaire Ingeniería S.A.S.

La tabla 14 evidencia la proyección financiera descrita en la sección de resultados.

Tabla 16. Proyección Financiera SGSI Indaire Ingeniería S.A.S.

PROYECCIÓN FINANCIERA DEL SGSI											
CONCEPTO	**FASE I** **DEFINICIÓN ALCANCE**	**FASE 2** **REDACCIÓN POLÍTICA DE SEGURIDAD**	**FASE 3** **EVALUACIÓN RIESGOS Y TRATAMIENTO RIESGOS**	**FASE 4** **REDACCIÓN DECLARACIÓN APLICABILIDAD**	**FASE 5** **IMPLEMENTACIÓN PROGRAMAS CAPACITACIÓN**	**FASE 6** **PUESTA EN MARCHA SGSI**	**FASE 7** **SUPERVISIÓN SGSI / AUDITORÍA INTERNA**	**FASE 8** **REVISIÓN DE GERENCIA**	**FASE 9** **CERTIFICACIÓN SISTEMA**	**FASE 10** **MANTENIMIENTO SGSI**	**DESCRIPCIÓN**
SEMANAS	**4 Semanas**	**8 Semanas**	**8 Semanas**	**4 Semanas**	**4 Semanas**	**8 Semanas**	**4 Semanas**	**2 Semanas**	**3 Semanas**	**8 semanas**	
Asesor interno	$ 2 000 000	$ 2 000 000	$ 4 000 000	$ 2 000 000	$ 2 000 000	$ 4 000 000	$ 2 000 000	$ 1 000 000	$ 1 500 000		Salario semanal $ 500 000
papelería	$ 13 000	-	-	-	$ 13 000	-	-	-	-	-	Resma de 500 Hojas
Medios Tecnológicos	$ 280 000	$ 280 000	$ 560 000	$ 280 000	$ 280 000	$ 560 000	$ 280 000	$ 140 000	$ 210 000		Alquiler Portatil $ 70 000 por semana
Asistente	-	-	$ 700 000	$ 700 000	-	$ 700 000	$ 700 000	-	$ 700 000	-	Salario semanal $ 175 000
Firewall Físico	-	-	$ 1 200 000	-	-	-	-	-	-	-	Equipo de protección recomendado
CCTV	-	-	$ 607 800	-	-	-	-	-	-	-	Equipo de protección recomendado
Antivirus	-	-	$ 350 000	-	-	-	-	-	-	-	Equipo de protección recomendado
Endpoint	-	-	$ 210 000	-	-	-	-	-	-	-	Equipo de protección recomendado
Control de acceso	-	-	$ 740 000	-	-	-	-	-	-	-	Equipo de protección recomendado
Detectores de humo	-	-	$ 168 000	-	-	-	-	-	-	-	Equipo de protección recomendado

Tabla 14. (Continuación).

Extintores	-	-	$ 320 000	-	-	-	-	-	-	-	Equipo de protección recomendado
UPS	-	-	$ 6 550 000	-	-	-	-	-	-	-	Equipo de protección recomendado
Polo a tierra	-	-	$ 300 000	-	-	-	-	-	-	-	Equipo de protección recomendado
Instalación de Equipos Tecnológicos	-	-	$ 3 000 000	-	-	-	-	-	-	-	Por concepto de instalación de equipo físico de protección
Capacitador	-	-	-	-	$ 2 000 000	-	-	-	-	-	Salario semanal $ 500 000
señalización	-	-	-	-	$ 450 000	-	-	-	-	-	Por concepto de señalización
Costo Certificación	-	-	-	-	-	-	-	-	-	-	Por concepto de certificación del sistema
Mantenimiento de Equipos Tecnológicos	-	-	-	-	-	-	-	-	-	$ 7 000 000	Costo aproximado de mantenimiento de equipos físicos.
COSTOS PARCIALES POR FASE	**$ 2 293 000**	**$ 2 280 000**	**$ 18 705 800**	**$ 2 980 000**	**$ 4 743 000**	**$ 5 260 000**	**$ 2 980 000**	**$ 1 140 000**	**$ 2 410 000**	**$ 7 000 000**	
COSTO TOTAL DE IMPLEMENTACIÓN DE SISTEMA ANUAL									**$ 49 791 800**		
OBSERVACIONES: El tiempo estimado para la implementación del sistema es aproximadamente un año. Se debe tener en cuenta que los tiempos de implementación de cada fase varían según lo estipule el asesor interno y la gerencia de la compañía.											

Anexo. 4. Cotizaciones recomendaciones físicas (Control de acceso y CCTV).

JD ASIA ELECTRONICS

JULIETTEH DIAZ REY

C.C.T.V • PILAS • TELEFONIA Y ACCESORIOS
UPS • ALARMAS • BIOMETRICOS • AUDIFONOS • RADIOS MOTOROLA
MEMORIAS USB SD • M2 • MP3 • Mp4 • CARGADORES • GRABADORAS

GP Panasonic MOTOROLA

COTIZACIÓN
Nº 4997

FECHA: 25 | 11 | 15

SEÑOR(ES):
NIT:
DIRECCIÓN:
TEL.

CANT.	DESCRIPCION	VR. UNIT.	VR. TOTAL
1	Control de acceso KAO	390000	
1	Electroiman 350 LBs	90000	
1	Boton no touch	65000	
1	Antirremanente	65000	
1	Fuente	85000	
1	Bateria 12v 7amp	~~45000~~	
		740000	
SON:		TOTAL $	

FIRMA CLIENTE
FIRMA VENDEDOR

CALLE 20 No. 8 - 96 • TEL. 282 3453 • Cel: 311 812 3443 • E-mail: julydiaz24@hotmail.com

IMPRESO POR PERFECTWORK NIT. 1023673038 - 1 CEL. 311 830 16 97

ElectroSeguridad Mundial

Sonido · Accesorios · Cableado · Video Vigilancia · Electrónico

SOLUSISTEMAS LTDA. NIT. 830.039.524-8 REGIMEN COMUN
Cra. 9 No. 20-58 Loc. 4 Tel: 243 9545 Fax: 243 3490 Bogotá, D. C. - contacto@solusistemascolombia.com

COTIZACION
Nº 947

FECHA: 25 | 11 | 15

SEÑOR(ES):
TELEFONO:
C.C. ó NIT.

CÓD.	ARTICULO	CANT.	V. UNIT.	V. TOTAL
	Dvr 4ch AHD	1	160000	160000
	Disco duro 1TB	1	125000	125000
	Camara domo 24 leds 2.8mm 1mpx sencial	4	69000	276000
	cable UTP		400	
	Video balun	4	6000	24000
	Baneros pc	4	3000	12000
	cajas de paso	4	2700	10800
	oferta – 1 Semana		SUBTOTAL	$
			IVA	$
			TOTAL	$

Garantia ___ meses, para efecto de garantia es ***INDISPENSABLE*** *presentar copia de la factura, el producto con todos sus accesorios y empaques originales. El sello de garantia debe estar en perfectas condiciones de lo contrario* ***LA GARANTIA SERA NULA****. la garantia no cubre daños ocasionados por desconfiguración, altos voltajes, golpes y/o mala manipulación del producto. Toda garantia* ***SIN EXCEPCIÓN*** *será resuelta en lapso de* ***CINCO (5) DÍAS HÁBILES*** *desde el momento de recibir el producto.*

VENDEDOR:

ESPECIALISTAS EN CIRCUITO CERRADO DE TV - ELECTRONICA
CABLEADO - SONIDO - TELEFONIA - PILAS Y BATERIAS
www.solusistemascolombia.com

Anexo. 5 Cotizaciones recomendaciones físicas (UPS y Detector de humo c/u).

CVT
CER VISION TECHNOLOGY

Carrera 9 No. 19 - 96
PBX 7560249
Ext. 106 - 107
cctv@cer.net.co
Bogotá D.C. - Colombia

COTIZACION
Nº 9582

Nit. 900422686-8
IVA Régimen Común

Este documento es valido únicamente como cotización

Señor(es) Indaire. Ingeniería.

Dirección | **Fecha** 25/11/15.

Teléfono | **NIT** | **Ciudad**

DESCRIPCION	Cantidad	Valor Unitario	VALOR TOTAL
Detector de humo.	1	28000	
UPS. ON LINE Nicomar. TITAN 6KVA (2 años de garantia).	1	6'550.000	
		IVA INCLUIDO.	

Garantía meses. Para efecto de garantía es **INDISPENSABLE** presentar copia de la factura, el producto con todos sus accesorios y empaques originales. El sello de garantía debe estar en perfectas condiciones, de lo contrario **LA GARANTÍA SERA NULA**. La garantía no cubre daños ocasionados por desconfiguración, altos voltajes, golpes y/o mala manipulación del producto. Toda garantía **SIN EXCEPCIÓN** sera resuelta en lapso de **OCHO (8) DÍAS HÁBILES** desde el momento de recibir el producto.

TOTAL A PAGAR $

Elaboró: Julieth

Observaciones:

PMS TP-LINK NICOMAR Videolink alhua HIKVISION D-TECH