DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN LA NORMA ISO 27001: 2013 PARA LA RED INALÁMBRICA DE LA EMPRESA INNOVACIÓN GLOBAL SAS UBICADA EN EL MUNICIPIO DE SIBUNDOY PUTUMAYO

DORIS ESTHER JOJOA PAZ

KAROL MARTIN CÓRDOBA CUAYCAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUTUMAYO, COLOMBIA
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN LA NORMA ISO 27001: 2013 PARA LA RED INALÁMBRICA DE LA EMPRESA INNOVACIÓN GLOBAL SAS UBICADA EN EL MUNICIPIO DE SIBUNDOY PUTUMAYO

DORIS ESTHER JOJOA PAZ

KAROL MARTIN CÓRDOBA CUAYCAL

Monografía como Trabajo de Grado presentado ante la Escuela de Ciencias Básicas, Tecnología e ingeniería (ECBTI) como parte de los requisitos para optar al Título Académico de Especialista en Seguridad Informática.

Director del proyecto

MSC. ARMANDO ARÉVALO MURILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUTUMAYO, COLOMBIA
2016

Nota de Aceptación:

_____

_____

_____

_____

Firma del Presidente Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SIBUNDOY DIA: MES: AÑO: 2016

DEDICATORIA

Dedico este trabajo a Dios por acompañarme en cada uno de mis pasos y darme la fortaleza para seguir adelante.

A mis padres y hermanos pilares de mi existencia, que constantemente me brinda su cariño y apoyo incondicional

A mi amigo Karol por brindarme su amistad y animarme a concluir este trabajo pese a todas las dificultades presentadas.

A la señora Fidelina y su esposo Jesús, por acogerme en su familia y apoyarme constantemente.

Finalmente dedico este trabajo a los tutores de la UNAD que me orientaron en los semestres de estudio. Gracias por ampliar mis conocimientos

Doris Esther Jojoa Paz

DEDICATORIA

Este proyecto se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. Todo este trabajo ha sido posible gracias a ellos.

A mis hermanos Sandra y Mario, y sobrinos Daniel, David y Kevin por estar siempre presentes acompañándome para poderme seguir adelante.

A Doris, quien ha sido mi mano derecha durante todo este tiempo; te agradezco por tu desinteresada ayuda, por darme una mano cuando siempre la necesité, por aportar considerablemente en este proyecto. Te agradezco no solo por la ayuda brindada, sino por los buenos momentos compartidos. Eres una gran persona, y me encanta tenerte a mi lado como una gran amiga.

Karol Martin Córdoba Cuaycal

AGRADECIMIENTOS

Los autores expresan sus agradecimientos:

Al señor Roberto Vallejo Santacruz gerente de la empresa Innovación Global SAS, por permitirnos realizar esta investigación y apoyarnos en las actividades que condujeron a la presentación de este proyecto.

Al ingeniero Ramsés Ríos Lampriello Líder Nacional del programa Especialización en Seguridad Informática, por su apoyo y supervisión en el proceso realizado para concluir este proyecto.

A nuestro director de proyecto, MSC. Armando Arévalo, por su paciencia, acompañamiento y oportunas orientaciones para el desarrollo de este proyecto.

Al Master en docencia Francisco Solarte Solarte, por compartir sus conocimientos y motivarnos en la finalización de este proyecto.

A la Universidad Nacional Abierta y a Distancia UNAD, por darnos la oportunidad de fortalecer nuestras competencias en el campo de la seguridad informática y ampliar nuestro horizonte como profesionales.

A todas aquellas personas que de una u otra forma nos acompañaron en el desarrollo de este proyecto y nos brindaron sus conocimientos.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ANEXOS

RESUMEN

En este proyecto se presentan las pautas a tenerse en cuenta para el diseño de un sistema de gestión de la seguridad informática (SGSI), basada en la norma ISO/IEC 27001:2013 y el anexo A ISO/IEC 27002:2013 que permiten determinar los controles de seguridad para la red inalámbrica de la empresa Innovación Global SAS, la cual presta el servicio de Internet en el municipio de Sibundoy Putumayo.

En el diseño del SGSI se tiene en cuenta el análisis de riesgos para los activos de información de la empresa, el cual se realiza siguiendo la metodología de Magerit en su versión 3 que permite evaluar los riesgos de los activos críticos de la empresa para mitigarlo. Posteriormente se presenta la declaración de la aplicabilidad teniendo en cuanta la norma ISO 27002:2013 y finalmente se presentan las políticas de seguridad resultante que concluyen este trabajo.

Palabras claves: SGSI, ISO 27001:2013, Magerit**,** Amenaza, declaración de aplicabilidad, políticas de seguridad.

ABSTRACT

In this project guidelines to be taken into account for the design of a management system of information security based on ISO / IEC 27001 (SGSI) are presented security controls for the wireless network company Global Innovation SAS, which provides Internet service in the town of Sibundoy Putumayo. In designing the SGSI it takes into account the analysis of risks to information assets of the company, which is carried out following the methodology Magerit in its version 3, which allows to evaluate the risks of critical business assets to mitigate it. Then are presented the declaration of the applicability taking into account the ISO 27002: 2013 and finally resultanting security policies that conclude this work.

Keywords: SGSI, ISO 27001:2013, Magerit, Threat, applicability statement, security policies

INTRODUCCIÓN

Hoy en día las redes de telecomunicación, se han convertido en el medio más utilizado para la comunicación de usuarios de todo el mundo y aunque es un medio efectivo para interactuar y acceder a la información, su uso se ha convertido en un desafío para la seguridad debido a las múltiples amenazas que han ido surgiendo y que cada vez son más complejas. Las amenazas se presentan cuando existe algún tipo de vulnerabilidad en la red que puede ser aprovechada, y que puede comprometer la seguridad de un sistema de información.

El aumento y evolución de las técnicas de ingeniería social, la falta de una capacitación adecuada y concientización a los usuarios en el uso de la tecnología, son algunas situaciones que llevan a un aumento en la aparición de amenazas.

Las vulnerabilidades que pueda tener la red de datos de una empresa o corporación, en muchas ocasiones pasan desapercibidas, y solo se nota cuando surgen problemas de seguridad que comienzan a afectar el funcionamiento de su entorno informático (Areitio Bertolín javier, 2009). Los ataques a los que puede verse expuesta una empresa aprovechando las vulnerabilidades en las que pueda incurrir debido a un deficiente sistema de seguridad, puede facilitar el acceso a uno de los activos más preciados de la empresa como es la información, afectar su prestigio y comprometer su credibilidad ante sus usuarios.

Por lo anterior proveer seguridad a la red en pro de la información que se maneja es una prioridad que toda empresa debe tener para ofrecer una adecuada continuidad en sus servicios. Hoy en día los proveedores del servicio de Internet (ISP) compiten con seguridad y los ISP que están dirigidos a los consumidores, además de internet también están obligados a ofrecer seguridad como parte de sus servicios.

.

1. TITULO DEL PROYECTO

Diseño de un Sistema de Gestión de Seguridad de La Información (SGSI) basado en la norma ISO 27001:2013 para la red inalámbrica de la empresa Innovación Global SAS ubicada en el municipio de Sibundoy Putumayo

1.1 TEMA

Gestión de la seguridad en las redes inalámbricas.

1.2 LÍNEA DE INVESTIGACIÓN

El proyecto se enmarca en el área de gestión de la información aplicada a la infraestructura tecnológica y seguridad en redes.

1.3 DELIMITACIÓN

La investigación se realizará en la empresa Innovación Global SAS, en el departamento del Putumayo, municipio de Sibundoy, teniendo en cuenta la red inalámbrica. Se realizara el estudio y análisis de la seguridad de la red para diseñar el SGSI acorde a las necesidades de la empresa; la implementación del Sistema de Gestión de Seguridad Informático quedará a cargo de la empresa.

2. DEFINICIÓN DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

Hoy en día las empresas se ven expuestas a diferentes riesgos y amenazas de seguridad, los cuales generalmente están dirigidos a los servicios que prestan, colocando en peligro la integridad, disponibilidad así como la confidencialidad de la información que se maneja en ella (Juan, 2014). Esta situación en la actualidad no solo aqueja a las grandes empresas sino que también se extiende a las pequeñas empresas, como Innovación Global SAS, la cual no es ajena a esta situación. Como una empresa que provee los servicios de internet mediante una red extendida y dispositivos de transmisión de datos inalámbrica o Wireless, en los últimos años se ha visto afectada por el acceso indebido de usuarios no autorizados, perdida de información, denegación del servicio, puntos de acceso caídos o con conflictos, ruidos y latencia entre otros, lo cual conllevan a una baja calidad en la prestación efectiva y eficiente de sus servicios y por ende usuarios insatisfechos. Por tal razón determinar las políticas de seguridad y controles pertinentes puede evitar la deserción de usuarios y que la imagen de la empresa decaiga, lo cual ocasionaría una gran pérdida económica y su mantenimiento en el mercado de las telecomunicaciones. Por tal razón el diseño de un Sistema de Gestión de Seguridad de la Información, teniendo en cuenta la norma ISO/IEC 27001:2013, para la red inalámbrica de la empresa, favorecerá gestionar eficientemente la accesibilidad de la información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información y así mismo minimizar los riesgos de seguridad que afronta como de aquellos que pueden surgir a corto o a largo plazo.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un SGSI ayudará a mejorar la seguridad en la red y el servicio a los usuarios garantizando la continuidad del servicio de la red inalámbrica de la empresa Innovación Global SAS en el municipio de Sibundoy Putumayo?

3. JUSTIFICACIÓN

La información es uno de los activos más importantes que posee toda empresa, por lo cual desarrollar mecanismos para asegurar la disponibilidad, integridad y confidencialidad en el manejo y manipulación de esa información es cada día más urgente; debido al avance de la tecnología, esta información hoy en día, está sujeta a muchas amenazas de carácter interno como externo. Por tal motivo tanto para la empresa grande como pequeña es necesario contar una eficiente seguridad para salvaguardarla de cualquier amenaza que le perjudique.

Para la red inalámbrica de Innovación Global, siendo esta el medio para proveer los servicios de internet en el municipio de Sibundoy y debido a problemas que se han venido presentando como: latencia entre enlaces, congestión en el espectro, desgaste en los equipos inalámbricos, conflictos de IP entre otros, conlleva a que se tomen medidas de seguridad para favorecer su desempeño y que se eviten riesgos que pueden perjudicar su funcionamiento como la información que se maneja en la red. La adopción de buenas prácticas le permitirán afrontar riesgos como: la denegación del servicio, el crakeo, la interferencia de transmisión o la intercepción de datos.

En la actualidad la empresa de Innovación Global, no cuenta con un Sistema de Gestión de Seguridad de la Información(SGSI), por lo cual está expuesta a numerosas fallas y vulnerabilidades que perjudican su funcionamiento y mantenimiento en el mercado; por lo cual un SGSI para esta empresa beneficiara en primera instancia al personal a cargo de la red porque presentaran menos problemas en ella, a la empresa en sí, porque se mejoraran sus servicios y la seguridad en la red, y finalmente a los usuarios porque podrán contar con un mejor servicio.

Un SGSI acorde a las necesidades de Innovación Global, teniendo en cuenta la norma ISO 27001:2013, le favorecerá a corto y largo plazo no solo en lo concerniente en su seguridad sino que también permitirá que se adopten buenas prácticas tanto para sus usuarios internos como externos y así pueda dar continuidad a sus servicios.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Mejorar la seguridad en la red y el servicio a los usuarios mediante el diseño de un SGSI garantizando la continuidad del servicio de la red inalámbrica de la empresa Innovación Global SAS en el municipio de Sibundoy Putumayo

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos informáticos de la empresa en cuanto a la red de datos y los servicios que presta a los usuarios para conocer su funcionamiento y las condiciones en que se encuentran.

- Identificar las vulnerabilidades y amenazas existentes para determinar los riesgos y hacer el análisis y evaluación de los riesgos

- Verificar la existencia de controles en la red de datos y los servicios que se prestan a los usuarios para determinar que controles existen y cuáles de ellos deberían implementarse.

- Diseñar las políticas de seguridad para la empresa Innovación Global SAS

5. MARCO REFERENCIAL

Para el desarrollo del presente proyecto se presenta los conceptos que se relacionan directamente con el tema, y que a la vez proveen de un soporte teórico que permite identificar definiciones para dar respuesta a los requerimientos propios del proyecto; la investigación de la temática que se involucra facilita realizar una secuencia lógica para el desarrollo de la propuesta como para el cumplimiento de los objetivos inicialmente mencionados.

5.1 ANTECEDENTES

Para esta investigación se tienen en cuenta los siguientes estudios previos relacionados con el diseño de un SGSI, los cuales se describen brevemente a continuación:

En el proyecto denominado "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO"[1] presentado por los estudiantes: Yezid Camilo Guerrero Angulo y Robert Marcelo Tabango. En el planteamiento del problema se describe que el manejo de controles de acceso físico aislados y no suficientes para la seguridad de la unidad informática y telecomunicaciones de la universidad de Nariño facilitan el acceso a los recursos que esta concierne, e igualmente se indica que el acceso de usuarios a la red inalámbrica sin ningún tipo de control debido a que no se cuenta con una adecuada configuración de la misma, no favorece el buen desempeño de la misma, por lo cual autores de la propuesta, sugieren un diseño de gestión de la seguridad de la información que permita corregir estas falencias para favorecer el adecuado funcionamiento de esta unidad como de fortalecer la seguridad de la red inalámbrica.

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

---

[1] GUERRERO, Angulo Yesid Camilo y TABANGO, Robert Goyes. "Sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad informática y telecomunicaciones de la universidad de Nariño". Tesis de grado para optar al título de ingeniero de sistemas. Pasto. Colombia. Universidad de Nariño.2014

Esta investigación se tiene en cuenta porque orienta el trabajo con respecto a los controles de la norma ISO 27001 y 27002, como de la metodología de MAGERIT para la evaluación de riesgos, que también se tienen en cuenta para esta propuesta.

En el proyecto de grado presentado por: Fernando Santiago Martínez, que se denomina "APOYO AL PROCESO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA ALCALDÍA DE PASTO BASADO EN LA NORMA ISO 27001:2013 Y BAJO LA DIRECTRIZ DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA VERSIÓN 3.1" [2]. En el planteamiento del problema se indica que la alcaldía de Pasto no cuenta con un SGSI, el cual es un requerimiento del Gobierno Nacional, quien ha implementado la estrategia del gobierno en línea para los organismos y entidades que conforman las ramas del poder público. Describe que la alcaldía no cuenta con un sistema de seguridad definido que permita respaldar con documentación suficiente los procesos que se desarrollan al interior de esta.

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

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

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

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

[2] MARTÍNEZ, Fernando Santiago. "Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información (SGSI) en la alcaldía de Pasto basado en la norma ISO 27001:2013 y bajo la directriz de la estrategia de gobierno en línea versión 3.1. Pasantía para optar el título de ingeniero de sistemas. Pasto, Colombia. Universidad de Nariño. 2015

5.2 MARCO TEÓRICO

En el marco teórico se tiene en cuenta la siguiente temática consultada:

5.2.1 La seguridad informática.

Consiste en asegurar que los recursos del sistema de información entre los cuales están el material informático o programa de una organización sean utilizados de la manera en que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.[3]

5.2.1.1 Principios de la seguridad informática.

Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

5.2.2 Amenazas, vulnerabilidades y riesgos

Los riesgos en la información se presentan cuando se denotan amenazas y vulnerabilidades, las cuales tiene una gran consecuencia. Las amenazas son situaciones que pueden afectar el funcionamiento de la empresa en lo referente a su sistema de información o al sistema que la procesa, mientras que las

[3] Gestión de Riesgo en la Seguridad Informática. ”La seguridad y sus principios”, tomado de https://protejete.wordpress.com/about/.

vulnerabilidades pueden determinarse como una debilidad en los procesos, la tecnología o infraestructura que tenga la empresa en su sistema informático.

5.2.2.1 Tipos de Amenazas (Seguridad informática- Tipo de amenazas).

Dependiendo del modo en que se presente el ataque, las amenazas pueden ser por origen, por efecto o por el medio utilizado. [4]

Amenazas por el origen. Teniendo en cuanta el origen del ataque y que en ocasiones no solo puede darse por internet sino que puede darse desde la misma empresa existen dos tipos de amenazas internas y externas.

- **Amenazas internas**, pueden causarse por personal de la empresa que tiene acceso a la red y cierto grado de privilegios que le permite acceder a la información de la empresa o el funcionamiento de sectores de cuidado. Otra amenaza interna, son las vulnerabilidades existentes en la red cuando no están debidamente protegidas tanto físicamente como lógicamente.

- **Las amenazas externas**, se producen fuera de la red, pueden ser prevenidas por el administrador de la red generalmente. Algunas de estas amenazas son: Virus, gusanos y caballos de Troya, Spyware y adware, ataques de día cero, ataques de piratas informáticos, ataques por denegación de servicio, interceptación y robo de datos, robo de identidad.

Amenazas por el efecto. Entre estas amenazas se presentan: Robo de información, destrucción de información, anulación del funcionamiento de los sistemas o efectos que tiendan a ello, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, robo de dinero, estafas.

Amenazas por el medio utilizado. Se pueden clasificar por el modo operante del atacante. Entre estas amenazas están: virus informáticos, phishing, ingeniería social, denegación de servicio, spoonfing de DNS, de IP, de DHCP

[4]Tipos de amenazas, tomado de : https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

5.2.2.2 Tipos de vulnerabilidades[5] (solarte, 2014)

Vulnerabilidad Física. Está a nivel del entorno físico del sistema, se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruirlo.

Vulnerabilidad Natural. Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales, que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del Hardware y del software: desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros, ya que depende del material que está construido. También hay sistemas que requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos. Ciertos fallos o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. Las vulnerabilidades en el software son conocidos como Bugs del sistema.

Vulnerabilidad de los Medios o Dispositivos. Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

Vulnerabilidad por Emanación. Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las Comunicaciones. La conexión de los computadores a redes supone, sin duda, un enorme incremento de la vulnerabilidad del sistema ya que aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También está el riesgo de intercepción de las comunicaciones, como la penetración del sistema a través de la red y la interceptación de información que es transmitida desde o hacia el sistema.

---

[5] Conceptos de Vulnerabilidad riesgo y amenaza tomado de: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

Vulnerabilidad Humana: la gente que administra y utiliza el sistema representa la mayor vulnerabilidad del sistema. Toda la seguridad del sistema descansa sobre la persona que cumple la función de administrador del mismo que tiene acceso al máximo nivel y sin restricciones al mismo. Los usuarios del sistema también suponen un gran riesgo al mismo.

5.2.2.3 Tipos de Riesgos (Riesgos Informáticos)

A continuación se describen algunos tipos de riesgos a los que puede enfrentarse la seguridad de un sistema informático[6]

Riesgos de Integridad. Entre este tipo de riesgos están: los de interface del usuario, procesamiento de errores, interface, administración de cambios, información

Riesgos de Relación. Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones.

Riesgos de acceso. En este tipo de riesgos están: procesos de negocio, aplicación, administración de la información, entorno de procesamiento, redes, nivel físico.

Riesgos en la infraestructura. Pueden presentarse por: Planeación organizacional, definición de las aplicaciones, administración de seguridad, operaciones de red y computacionales, administración de sistemas de bases de datos o información/negocio

Riesgos de seguridad general. Pueden ocasionarse por choques de eléctricos, incendio, niveles inadecuados de energía eléctrica, riesgos de radiaciones, mecánicos

Concentración de procesamiento de aplicaciones más grandes y de mayor complejidad. Una de las causas más importantes del incremento en los riesgos

[6]"Riesgos informáticos tomado de :" http://audisistemas2009.galeon.com/productos2229079.html

informáticos probablemente sea el aumento en la cantidad de aplicaciones o usos que se le da a las computadoras y la consecuente concentración de información y tecnología de software para el procesamiento de datos.

Dependencia en el personal clave. La dependencia en individuos clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone a la compañía en manos de relativamente pocas personas, siendo que éstas por lo general son externas a la organización.

5.2.3 Norma ISO 27001[7].

Es una norma que puede ser implementada en organizaciones o empresas con o sin a ánimo de lucro, privada o pública, pequeña o grande, la cual permite implementar la gestión de seguridad de la información, así como la certificación de la empresa. Esta norma internacional fue emitida por la Organización Internacional de Normalización (ISO) y en ella se describe la forma de gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Qué es ISO 27001?)

Figura 1. Estructura ISO 27001

Fuente: los autores

[7] Que es ISO?. Tomado de http://www.iso27001standard.com/es/que-es-iso-27001/

Mediante la implementación de la norma ISO 2001 se protege la confidencialidad, integridad y disponibilidad de la información de la empresa o corporación; por lo cual es necesario investigar los problemas que perjudican la información y la forma como se deben tratar y evaluar los riesgos, ante los cuales se enfrenta. En cuanto a los controles que se deben implementar se tienen en cuenta políticas de seguridad, procedimientos como la implementación técnica, la cual puede ser bien de software o de equipos. Esta norma es útil para determinar las reglas necesarias para prevenir instrucciones a la seguridad de un sistema informático. La ISO 27001 puede favorecer a las empresas en los siguientes beneficios: cumplimiento en requerimientos legales, valor agregado, menores costos, mejor organización, eficacia en su funcionamiento.

5.2.3.1 Controles de la norma ISO 27001:2013[8]

La ISO 27001 está conformada por 14 dominios y 114 controles y 130 requisitos de gestión. A continuación se presenta un resumen general de algunos de los controles de esta norma.

- **Gestión de activos**: Tiene en cuenta la identificación de los activos de información de la empresa, los requerimientos de los activos para su confidencialidad, integridad como disponibilidad.

- **Política de seguridad:** Documento mediante el cual se indican las pautas a tenerse en cuenta para la seguridad de la información de la empresa Ingenio Global.

- **Organización de la seguridad:** hace referencia a la estructura de seguridad que se tendrá en cuenta para determinar la seguridad de la información dentro de la empresa. Se tienen en cuanta los roles de los usuarios internos como externos, los compromisos, acuerdos, autorizaciones, entre otros.

- **Seguridad del Recurso Humano:** Tiene en cuenta los roles del personal de la empresa sus usuarios, determinando responsabilidades, así como los riesgos relacionados dicho personal.

- **Seguridad Física y del entorno:** se tiene en cuenta los controles y los procedimientos para prevenir el acceso físico que no está autorizado, las

[8] Resumen realizado tomando como referencia a lo expuesto en: Compendio SGSI. Segunda edición. “Noma técnica Colombiana NTC-ISO/IEC 27001.Bogotá D.C. 2009

interferencias, los daños en las instalaciones de la empresa como de su información.

- **Comunicaciones y operaciones:** tiene en cuenta procedimientos y controles para la adecuada operación del entorno de la información.

- **Control de acceso e incidentes de seguridad:** Concierne los procedimientos y controles que garantizaran el acceso a los activos de información de forma restringida al personal autorizado como a los controles y procedimientos para la identificación de eventos de seguridad de la información y debilidades relacionadas con los sistemas de información, con el fin de comunicar esta deficiencia para que se tomen acciones correctivas adecuadas.

5.2.4 ISO 27002[9]

La ISO 27002 (no certificable) es el Anexo A de la ISO 27001, además es considerada un Código de buenas prácticas para la gestión de la seguridad de la información. La ISO/IEC 27002:2013, describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios.

Los dominios que agrupan los controles de esta norma son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Cifrado
- Seguridad física y ambiental
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Adquisición y mantenimiento de los sistemas de información
- Relaciones con suministradores
- Gestión de incidentes en la seguridad de la información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.
- Cumplimiento

[99] Apuntes tomados de : Norma Técnica Colombiana NTC-ISO 27002. Bogotá.2010

5.2.5 Sistema de Gestión de la Seguridad de la Información (SGSI)

Se considera como un sistema de gestión de seguridad de la información que implementa los procesos que permiten que una organización realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales; con el fin de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente, adaptada a los cambios que se produzcan en el entorno y las tecnologías.[10]

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio-ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS 18001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización. (López Neira Agustín, 2012).

Figura 2. Proceso de evaluación del riesgo

Fuente: http://www.iso27000.es

[10] Manuel, Fernández Carlos.(2012).La norma ISO 27001 y el Sistema de Gestión de la seguridad de la información.

5.2.5.1 La importancia del SGSI

Un sistema de gestión de la seguridad de la información es de gran importancia por cuanto permite la administración relacionada con la seguridad de la información, que es un aspecto fundamental importante de una, su adopción implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Figura 3. Ciclo de vida continúo PHVA

Fuente: los autores

5.2.6 El ciclo continúo PDCA o PHVA

Para implementar y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA. Figura 3, este ciclo es tradicional en los sistemas de gestión de la calidad. [11]

Su aplicación consta de cuatro etapas, que se mencionan a continuación:

Plan (planificar): establecer el SGSI.
Do (hacer): implementar y utilizar el SGSI.
Check (verificar): monitorizar y revisar el SGSI.
Act (actuar): mantener y mejorar el SGSI.

Planificar. se tiene en cuenta: definir el alcance del SGSI en términos del negocio, definir una política de seguridad, definir una metodología de evaluación del riesgo, identificar los riesgos, analizar y evaluar los riesgos, Identificar y evaluar las distintas opciones de tratamiento de los riesgos, seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del

[11] Norma técnica Colombiana NTC-ISO/IEC 2700. “El modelo PHVA aplicado a los procesos de SGSI”. 2009

riesgo, aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI y definir una declaración de aplicabilidad.

Hacer. se tienen en cuenta: definir un plan de tratamiento de riesgos, implantar el plan de tratamiento de riesgos, implementar los controles, Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles, procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal, gestionar las operaciones del SGSI, gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información, implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Verificar. Se tienen en cuenta: ejecutar procedimientos de monitorización y revisión, revisar regularmente la efectividad del SGSI, medir la efectividad de los controles, revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, realizar periódicamente auditorías internas del SGSI, revisar el SGSI por parte de la dirección, actualizar los planes de seguridad, registrar acciones y eventos.

Actuar. Se tienen en cuenta: implantar en el SGSI las mejoras identificadas, realizar las acciones preventivas y correctivas, Comunicar las acciones y mejoras, asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

5.2.7 MAGERIT

“MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de lo s Sistemas de información de las Administraciones Públicas”. Es un método de carácter público elaborado por el Consejo Superior de Informática (CSI), órgano del Ministerio de Comunicaciones de Administraciones Públicas (MAP), que se encarga de la preparación elaboración, desarrollo y aplicación de la política informática del gobierno Español.

Este método nace para minimizar los riesgos asociados al uso de sistemas informáticos y telemáticos, garantizando la autenticación, confidencialidad, integridad y disponibilidad de dichos sistemas y generando de este modo confianza en el usuario de los mismos”[12]

[12] MAGERIT. Consultada en file:///D:/magerit/Seguridad%20Informatica%20-%20MAGERIT.html

5.2.7.1 Objetivos de Magerit

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.

- Ayudar a descubrir y planificar las salvaguardas oportunas para mantener los riesgos bajo control.

- Apoyar a la Organización en la preparación de procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

A nivel conceptual, MAGERIT se basa en la evaluación y relación lógica de los siguientes conceptos:[13]

Figura 4. Magerit

Fuente: http://calidadtic.blogspot.com.co/2014/02/gestion-del-riesgo.html

Como se puede observar en la figura 3. El análisis de riesgos gira entorno a los conceptos de:

[13] Gestión del riesgo. Recuperada de: http://calidadtic.blogspot.com.co/2014/02/gestion-del-riesgo.html

Activo: elemento que tiene un valor para la organización
Amenaza: acontecimiento que supone un impacto negativo sobre el activo y
Salvaguarda: medida implantada para proteger el propio activo

Los objetivos principales son:

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.
- Determinar a qué amenazas están expuestos dichos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia

5.2.7.2 Estructuración de Magerit[14]

MAGERIT está estructurado en tres partes diferenciadas así:

Libro I: Método.
Libro II: Catálogo de Elementos.
Libro III: Guía de Técnicas.

El método. Comprende la Planificación del Análisis y Gestión de Riesgos y el análisis de riesgos

Catálogo de Elementos. Ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

Guía de técnicas. Proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos.

---

14 http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vw_TGzB97IU

5.2.8 La seguridad inalámbrica[15]

La seguridad es de gran importancia cuando de implementar redes inalámbricas se trata, por lo cual tener un conocimiento de los elementos de la seguridad de LAN inalámbricas, así como el uso de buenas prácticas puede ayudar a beneficiarse de las ventajas de las redes inalámbricas. A continuación se indican tres acciones que se pueden realizar para proteger este tipo de red.

- **Proteger los datos durante su transmisión mediante el cifrado.** El cifrado es como un código secreto. Traduce los datos a un lenguaje indescifrable que sólo el destinatario indicado comprende. El cifrado requiere que tanto el remitente como el destinatario tengan una clave para decodificar los datos transmitidos. El cifrado más seguro utiliza claves muy complicadas, o algoritmos, que cambian con regularidad para proteger los datos.

- **Desalentar a los usuarios no autorizados mediante autenticación:** los nombres de usuario y las contraseñas son la base de la autenticación, pero otras herramientas pueden hacer que la autenticación sea más segura y confiable. La mejor autenticación es la que se realiza por usuario, por autenticación mutua entre el usuario y la fuente de autenticación.

- **Impedir conexiones no oficiales mediante la eliminación de puntos de acceso dudosos:** un empleado bienintencionado que goza de conexión inalámbrica en su hogar podría comprar un punto de acceso barato y conectarlo al zócalo de red sin pedir permiso. A este punto de acceso se le denomina dudoso, y la mayoría de estos puntos de acceso los instalan empleados, no intrusos maliciosos. Buscar la existencia de puntos de acceso dudosos no es difícil. Existen herramientas que pueden ayudar, y la comprobación puede hacerse con una computadora portátil y con software en un pequeño edificio, o utilizando un equipo de administración que recopila datos de los puntos de acceso.

5.2.8.1 Soluciones de seguridad inalámbrica

Para proteger el cifrado y la autenticación de LAN inalámbrica, se puede realizar mediante un Acceso protegido Wi-Fi (WPA), Acceso protegido Wi-Fi 2 (WPA2) y conexión de redes privadas virtuales (VPN). Estas soluciones se tienen en cuanta

[15] Información obtenida de : http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

de acuerdo a un tipo específico de LAN inalámbrica a la que se desea acceder como a su nivel de cifrado de datos.[16]

WPA y WPA2: estas certificaciones de seguridad basadas en normas de la Wi-Fi Alliance para LAN de grandes empresas, empresas en crecimiento y para la pequeña oficina u oficinas proporcionan autenticación mutua para verificar a usuarios individuales y cifrados avanzados. WPA proporciona cifrado de clase empresarial y WPA2, la siguiente generación de seguridad Wi-Fi, admite el cifrado de clase gubernamental. WPA o WPA2 es una buena opción para las implementaciones de LAN inalámbrica para grandes y pequeñas empresas, estas certificaciones de seguridad favorece un control de acceso seguro, cifrado de datos robusto y protegen la red de los ataques pasivos y activos.[17]

VPN: VPN brinda seguridad eficaz para los usuarios que acceden a la red por vía inalámbrica mientras están de viaje o alejados de sus oficinas. Con VPN, los usuarios crean un "túnel" seguro entre dos o más puntos de una red mediante el cifrado, incluso si los datos cifrados se transmiten a través de redes no seguras como la red de uso público Internet. Los empleados que trabajan desde casa con conexiones de acceso telefónico o de banda ancha también pueden usar VPN.

5.3 MARCO CONCEPTUAL

En esta sección se presentan la terminología, que se tendrán en cuenta para la documentación del proyecto.[18]

SEGURIDAD INFORMÁTICA. Es el conjunto de los procedimientos estrategias y herramientas que permiten garantizar la integridad, la disponibilidad y confidencialidad de la información de una entidad.

AMENAZAS. Son posibles ocurrencias de un evento o acción que pueden causar grandes daños a un sistema informático.

---

[16] CUÉLLAR, Ruiz Jaime. Redes Inalámbricas .Estándares y mecanismos de seguridad.http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

[17] Soluciones de seguridad inalámbrica. Recuperado de: http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

[18] Definiciones en el contexto de los sistemas de gestión de seguridad de la información. Consultados en: http://www.iso27000.es/glosario.html

VULNERABILIDADES. Se determinan como las debilidades que puede tener un sistema informático, y que de no controlarse pueden atentar contra la confidencialidad, integridad, disponibilidad y autenticidad de la información de una empresa.

RIESGO. Según la Organización Internacional (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños"

ACTIVOS. Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes las, comunicaciones y la información en sí misma.

IMPACTOS. Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.

CONFIDENCIALIDAD: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

INTEGRIDAD: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

DISPONIBILIDAD: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

SGSI (Sistema de Gestión de la Seguridad Informática). Es un proceso sistemático, documentado que se realiza para garantizar que la seguridad de la información es gestionada correctamente, para contrarrestar los riesgos a los cuales puede estar expuesta la empresa.

ANÁLISIS DEL RIESGO. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [19]

[19] Guía ISO/IEC 27013:2013

DECLARACIÓN DE LA APLICABILIDAD. Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

EVALUACIÓN DEL RIESGO. Proceso de comparar el riesgo estimado contra criterios de riesgos dados, para determinar la importancia del riesgo. [Guía ISO/IEC 73:2002]

ANÁLISIS DE RIESGOS. Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.
EVALUACIÓN DE LOS RIESGOS. Proceso en el que se coteja el riesgo estimado contra los criterios de la organización para determinar la importancia del riesgo.

TRATAMIENTO DE RIESGOS. Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

5.4 MARCO LEGAL

En este punto se indican las leyes y artículos que rigen el uso de las redes y las telecomunicaciones.[20].

Ley 1266 de 2008. Mediante esta ley se indican las disposiciones generales del hábeas data que se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros. Esta ley se refiere a que todo individuo puede conocer, actualizar y rectificar toda información que se relacione con él, la cual se encuentra almacenada en centrales de información. (Ley Estatutaria 1266 de 2008, 2008)

Ley 1341 de 2009. En esta ley se determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones(TIC), el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la

[20] CABRERA, Meza Harold Emilio. MODULO_208020_2013 telecomunicaciones. UNAD.2013

inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información (Ley 1341 de 2009, 2012)

Ley 527 de Agosto de 1999 Comercio electrónico. Por medio del cual se define y reglamenta el acceso y usos de los mensajes de datos del comercio electrónico y de las firmas digitales y se establece las entidades de la certificación y se dictan otras disposiciones. (Ley 527 de 1999)

Ley 1273 de 2009. Hace referencia a la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones: [21]

Artículo 269A: Acceso abusivo a un sistema informático. Hace referencia a que se acceda sin autorización en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269b: obstaculización ilegítima de sistema informático. Se refiere a la obstaculización para el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

---

[21] Ley 1273 de 2009. Recuperada de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Ley 1266 de 2008. Define el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Por lo cual se obliga a las empresas a que tengan un mayor cuidado con el manejo de datos personales de todo su personal; esta ley obliga a que se tenga una autorización para sustraer o interceptar dichos datos a pedir autorización al titular de los mismos.[22]

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. (protección de la información y de los datos)

[22] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

6. METODOLOGÍAS

6.1 METODOLOGÍA DE LA INVESTIGACIÓN

La metodología de la investigación de este proyecto es de tipo cuantitativo y descriptivo. Cuantitativo por cuanto se realizara la medición de algunas variables de la seguridad de la información y descriptivo porque se describen cada uno de los activos de información como procesos y servicios que se prestan.

6.2 POBLACIÓN

Para la población se tiene en cuenta el personal a cargos de la red (Administradores y técnicos).

6.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de la información se tiene en cuanta la entrevista al personal a cargo de la red, la observación directa, registro fotográfico de los equipos, información adicional encontrada de la empresa, fuentes documentales respecto a: diseño de un SGSI, Norma ISO 27001 y 27002, metodología de MAGERIT, entre otras temáticas de interés para este trabajo.

6.4 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Pasos a seguirse para el cumplimiento de los objetivos propuestos:

En primera instancia se tendrá en cuenta el cumplimiento con el primer objetivo de esta investigación (Identificación de los activos informáticos de la empresa) donde se realiza un reconocimiento de la infraestructura física y tecnológica de Innovación Global, para su cumplimiento se procederá a lo siguiente:

- Visita a la empresa para realizar un reconocimiento de sus servicios, infraestructura tecnológica de la red, infraestructura organizacional.
- Entrevista al administrador de la red y técnicos respecto a la seguridad de los activos de información.
- Hacer el registro fotográfico de la ubicación de antenas y equipos de red existentes en la empresa

En un segundo paso, se tienen en cuenta el segundo objetivo (Identificación de vulnerabilidades y amenazas de la red de Innovación Global) el cual involucra:

- Análisis de la situación actual de la empresa teniendo en cuenta los registros fotográficos realizados en la empresa, el resultado de la entrevista, la observación de la funcionabilidad de los equipos y la red y atención al usuario entre otros.

- Realización de pruebas de pentesting para identificar vulnerabilidades en la red y posibles amenazas que pueden poner en riesgo el sistema de información de la empresa.

- Aplicar la metodología MAGERIT para hacer la valoración de vulnerabilidades y amenazas en los activos informáticos.

En el tercer paso, se realizara la Verificación de la existencia de controles en la red de datos donde se realizara lo siguiente:

- Verificación de controles existentes que aplican la norma 27002, mediante un checklist.

- Declaración de aplicabilidad. Selección de los dominios y controles de la norma ISO 27002, para contrarrestar las amenazas encontradas

Finalmente con la información obtenida de los pasos anteriores se procederá a realizar el diseño de las políticas de seguridad para Innovación Global

7. DESARROLLO DEL PROYECTO

7.1 DESCRIPCIÓN DE LA EMPRESA

INNOVACIÓN GLOBAL SAS, es una empresa joven conformada por un equipo muy eficiente de profesionales en el Área de Sistemas y contabilidad y finanzas. Esta empresa presta el servicio de internet en el municipio de Sibundoy, la cual cuenta con una red extendida en todo el municipio, por medios de dispositivos de transmisión de datos inalámbrica o Wireless.

Innovación Global SAS. Cuenta con una licencia del Ministerio de Tecnologías de la Información y Comunicación según resolución No. 010905. Su buena atención, prestación de servicios a precios cómodos, la han llevado a ser la mejor empresa prestadora del servicio de internet, constituyéndose como la número uno en Sibundoy.

Misión. Proveer a los usuarios un servicio de internet que cumplan con sus expectativas, a un costo competitivo en el mercado, de tal forma que represente un ahorro en materia económica y una ventaja en términos de calidad, logrando satisfacer las necesidades establecidas.

Visión. Ser reconocida como una empresa prestadora de servicio de internet líder en el municipio de Sibundoy y asegurar una competitividad sostenible y rentable permanentemente.

7.1.1 Reseña Histórica

Innovación Global SAS, inicialmente inicia sus labores en el año 2006, en el municipio de Sibundoy Putumayo con el nombre de Ingenio Global Ltda. Posteriormente el 28 de enero del 2015, cambia su nombre por INNOVACIÓN GLOBAL SAS, según matricula mercantil No. 54309-16.

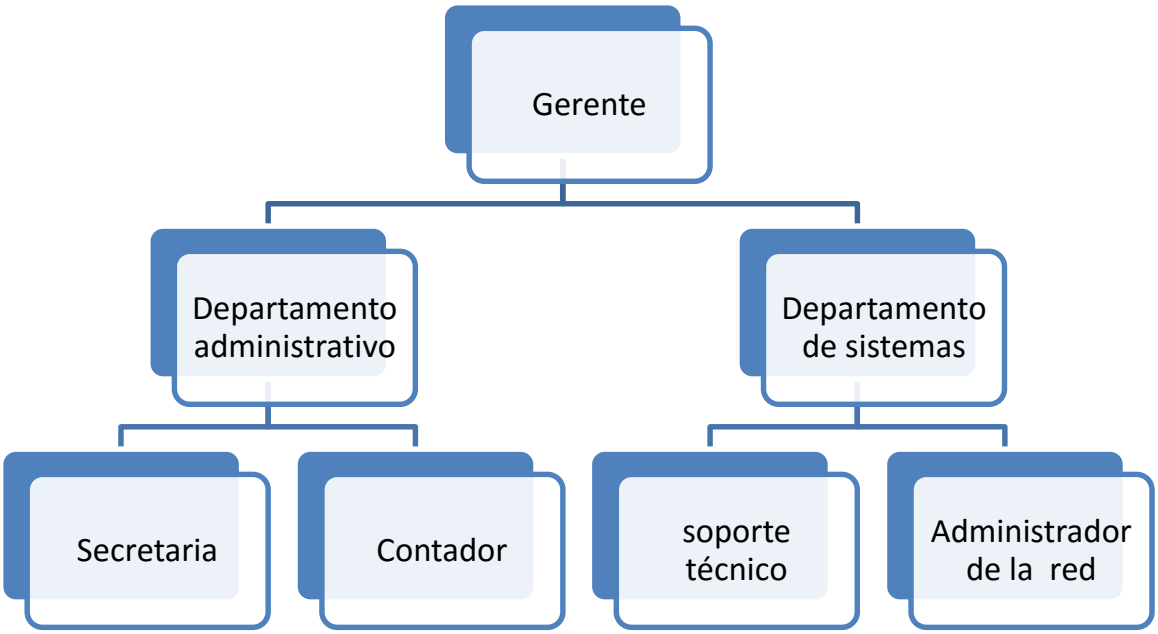
La empresa fue fundada por el señor Roberto Vallejo Santacruz y su Hijo Roberto Javier Vallejo, quienes vieron la necesidad de que en el municipio de Sibundoy era

necesario contar con un servicio de internet domiciliario. En sus inicios se constituyó como la segunda empresa que prestaba el servicio de internet en Sibundoy después de la empresa de DMG Conexiones a cargo del señor Javier Ponce.

7.2 ESTRUCTURA INSTITUCIONAL

Innovación Global SAS, se estructura de la siguiente forma para su funcionamiento: Gerente general, departamento administrativo, departamento de facturación y departamento de sistemas.

Figura 5. Diagrama Organizacional de Innovación Global SAS



Fuente: Información obtenida de Innovación Global SAS

7.2.1 Descripción de departamentos

7.2.1.1 Departamento administrativo.

Está conformado por el contador y la secretaria general. La secretaria se encarga de llevar el control de la facturación del servicio a usuarios, validando reportes mes a mes y hacer entrega de la respectiva factura; también atiende las solicitudes de los servicios de los usuarios, los informes respectivos de la facturación generada es entregada al contador para que la procese. A su vez la persona a cargo de la contabilidad realiza la elaboración de balances generales, administración de finanzas, control de impuestos, nómina, inventario.

7.2.1.2 Departamento de sistemas

Se encarga de llevar un control de usuarios, administración del ancho de banda, soporte técnico a usuarios y monitoreo de la red e instalación. Las funciones del administrador de la red y del personal técnico se indican a continuación:

Funciones del administrador de la red

- Administrar las redes inalámbricas de comunicación
- Administrar el servicio de internet.
- Administrar los sistemas de monitoreo y seguridad de los equipos de comunicación y los servicios de red.
- Evaluar y proponer nuevas tecnologías y servicios relacionados con redes inalámbricas de comunicación.
- Analizar, diseñar y evaluar topologías de redes inalámbricas físicas y lógicas para la empresa.
- Promover y gestionar mejoras en la infraestructura tecnológica que aseguren el buen funcionamiento y desempeño de la red inalámbrica con que cuenta la empresa, y que al mismo tiempo satisfagan los requerimientos de los usuarios.
- Mantener un inventario actualizado de todos los equipos y recursos informáticos de la empresa.

Funciones del personal técnico

- Instalar y dar mantenimiento a la red inalámbrica.
- Brindar asesoría técnica en el área de redes inalámbricas y comunicación a los usuarios en general.
- Instalar los equipos informáticos relacionados con la red inalámbrica y elementos de conectividad para garantizando su buen funcionamiento.
- Efectuar las reparaciones que se requieran en los equipos informáticos relacionados con la red inalámbrica de acuerdo a los procedimientos establecidos.
- Mantener en condiciones óptimas la red inalámbrica de comunicaciones para el servicio de internet.
- Ofrecer asesoría y asistencia técnica en caso de fallo en usuarios e infraestructura.

7.3 SERVICIOS

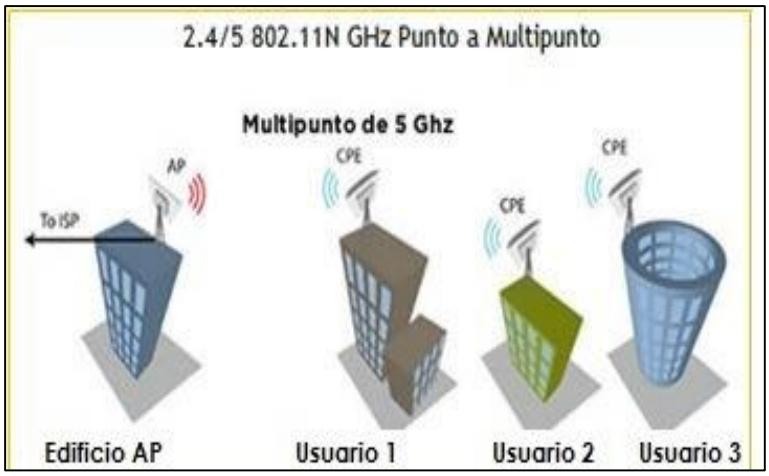
La empresa Innovación Global, presta el servicio de internet en el municipio de Sibundoy Putumayo, el cual funciona de acuerdo a las necesidades del usuario, ofreciendo soporte técnico y garantía del servicio sin cláusulas de permanencia, la única condición es el pago de instalación y equipos de red de datos para el usuario. A continuación se indica el tipo de servicio de internet para sus tres tipos de usuario

Usuario 1: internet para el hogar 1 megabytes.
Usuario 2: internet para empresas u otra entidades 2 a 3 megabytes.
Usuario 3: internet para entidades gubernamentales o dependiendo de la exigencia de la entidad 6 megabytes.

Costos de Los Servicios. El precio por el servicio de internet se está valorizado $40.000 pesos en el valor de inscripción y $30.000 pesos el valor mensual sin cláusulas de permanencia y si sus requerimientos fueran mayores se incrementa entre $80.000 y $35.000 pesos mensuales.

Tipo de Conexión. Las soluciones de Innovación Global permiten ofrecer tecnologías de conectividad punto a multipunto (PMTP) inalámbrico que garantizan alta disponibilidad, estas pueden trabajar bajo estándares 802.11a / g y IEEE 802.11n que proporcionan un rendimiento mayor a (802.11a / g). El objetivo primario de los multipuntos es la transmisión de datos, pero también puede transmitir VoIP. Los dispositivos el AP y CPE (Figura 6), es decir la estación de trabajo están equipados con antenas de polarización dual que incrementan la confiabilidad, su frecuencia son de 2.4 Ghz y 5Ghz con un amplio alcance.

Figura 6. Tipo de conexión



Fuente: empresa Innovación Global SAS

7.3.1 Ancho de banda y características de la red inalámbrica

El ancho de banda asignado de acuerdo al tipo de usuario se indica en la tabla 1.

Tabla 1. Ancho de banda según tipo de usuario

TIPO DE USUARIO	ANCHO DE BANDA	REÚSO ANCHO DE BANDA
Usuario 1	1 megabytes	½
Usuario 2	2 a 3 megabytes	½
Usuario 3	6 megabytes	½

Fuente: Empresa Innovación Global

A continuación se indica las características principales de la red inalámbrica de Innovación Global SAS. Tabla 2.

Tabla 2. Características de la red inalámbrica de Innovación Global

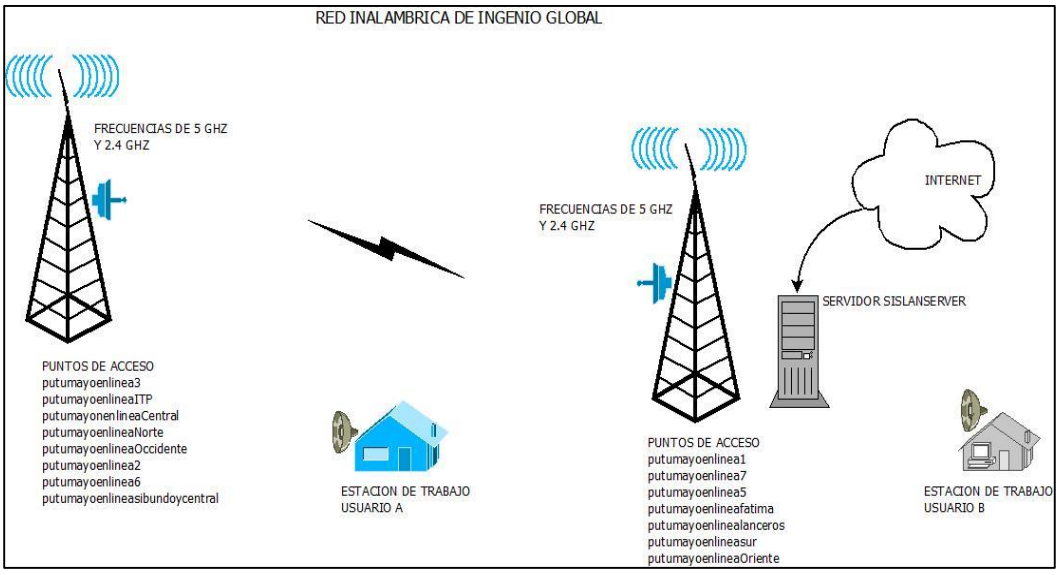
CARACTERÍSTICAS	RED INALÁMBRICA
Componentes físicos de la red	Access Point y estación de trabajo inalámbrico, router inalámbrico.
Costo comparativo	Costo moderado
Velocidad de transferencia	Puede variar entre 120 a 150 mbps
Alcance	Diámetro de alcance aproximado de señal de 2 a 3 kilómetros.
Ventajas	Alta movilidad para equipos y Fácil para incorporar nuevos clientes.

Fuente: Empresa Innovación Global

7.4 SISTEMA INFORMÁTICO DE INNOVACIÓN GLOBAL SAS

A continuación se presenta el diagrama de la red inalámbrica de la empresa de Innovación Global. Figura 5.

Figura 7. Diagrama de la red inalámbrica de Innovación Global



Fuente: Los autores

La empresa Innovación global cuenta con un canal dedicado con un reusó de 1/1 de fibra óptica, posee un solo proveedor; aunque su sistema está diseñado para el balanceo de carga no lo necesita por el momento ya que es un solo canal con la capacidad de 100 megabytes.

Actualmente tiene 150 usuarios y según los criterios de evaluación se puede extender a 200 usuarios.

7.5 RESUMEN INFORMATIVO Y FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN SENSIBLES

7.5.1 Servidor Sisland Server 12.12

Consiste en un software que permite administrar, controlar y optimizar el servicio de internet en toda la red; este se instala como sistema operativo en un computador de mediana potencia y opera como un router/servidor potente que optimiza el ancho de banda, puede controlar hasta 800 clientes a través del mismo.

Se compone principalmente de dos paquetes de software:

El sistema operativo Ubuntu Linux Server y ABC, que es el sistema de control y configuración del servidor que permite aprovechar toda la potencia de la plataforma Linux Ubuntu sin necesidad de conocimientos avanzados o costosas configuraciones a medida.

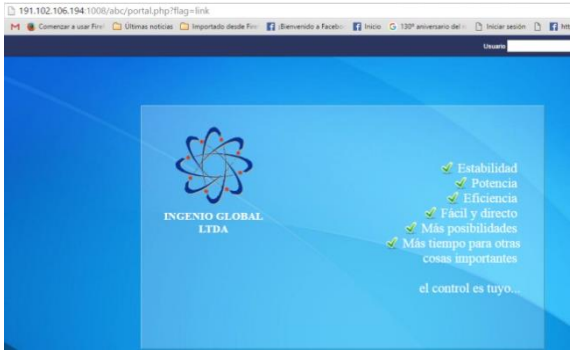
ABC ha sido diseñado y programado a partir de los requerimientos de administradores de ISP, cybers, instituciones educativas, oficinas públicas, entre otros, que necesitaban controlar el ancho de banda que utilizaban sus usuarios.

No sólo limita el consumo de cada usuario sino que realiza una distribución optimizada del mismo, aplicando complejos algoritmos de cálculo, además, dispone de una interfaz web muy trabajada que hace aún más fácil la tarea del administrador de la red.

Para acceder a dicha interfaz puede utilizarse cualquier navegador desde la red interna o desde internet, si el servidor tiene IP pública la URL es:

http://191.102.106.194:1008/abc/portal.php?flag=link tal como se muestra en la figura 8.

Figura 8. Servidor Sisland Server



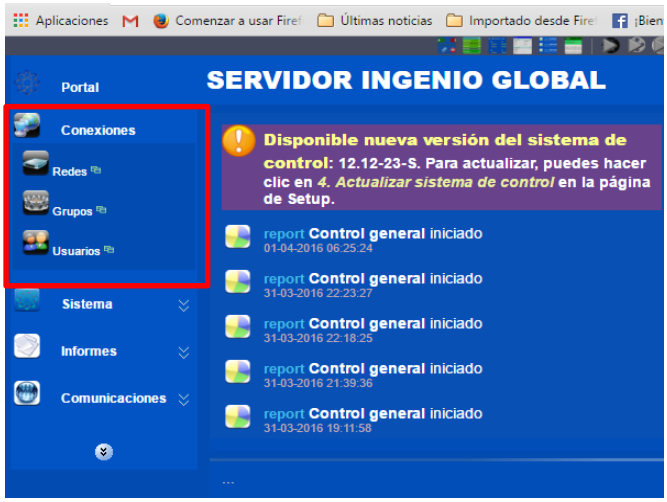
Fuente: servidor de Innovación Global

El módulo principal de ABC le ofrece el control completo del acceso y del ancho de banda y una base sólida para incorporar módulos adicionales con mayores prestaciones como balanceo de conexiones a internet, bloqueo de puertos, estadísticas gráficas, navegación prepaga entre otros.

CATEGORÍAS. A través de estos íconos se accede a las diferentes categorías que agrupan todas las páginas que componen el sistema:

CONEXIONES. Redes, Grupos y Usuarios, componen esta categoría es la más usada frecuente y se muestra en la figura 9.

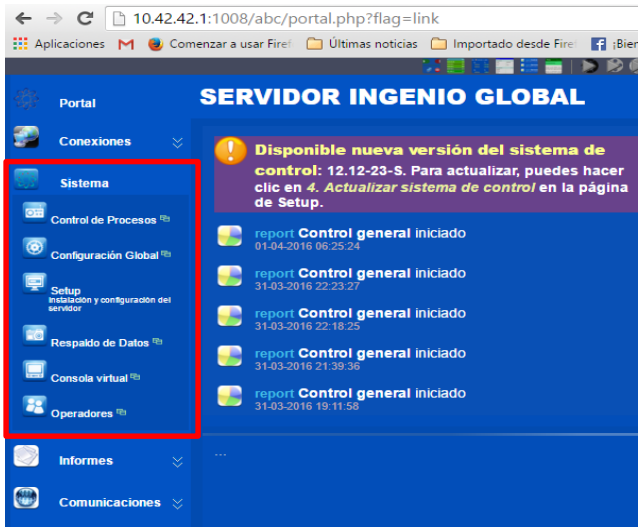
Figura 9. Conexiones Sisland Server



Fuente: Servidor Innovación global

SISTEMA. Son páginas con funciones estructurales como control de procesos, configuraciones generales, respaldo y recuperación de datos, entre otros y se muestra en figura 10.

Figura 10. Sistema en Sisland Server



Fuente: Innovación Global

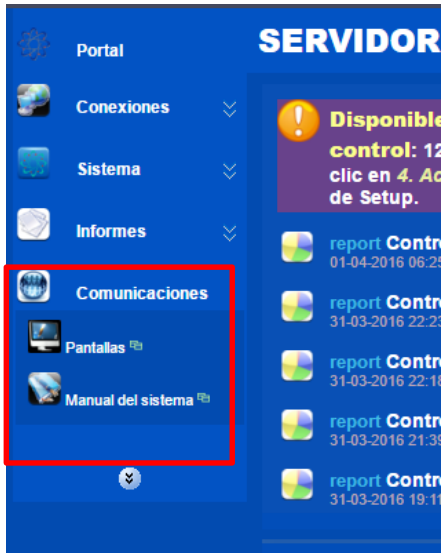
INFORMES. Es el acceso a páginas con información variada sobre el sistema y el consumo del ancho de banda y se muestra en la figura 11.

Figura 11. Informes Sisland server

Fuente: Innovación Global

COMUNICACIONES. Es el acceso a un manual y a otras páginas como el enlace para volver al portal. Figura 12.

Figura 12. Comunicaciones Sisland Server



Fuente: Innovación Global

Sisland Server permite ver todas funcionalidades de la red inclusive crea su propio diagra de red tal como se muestra en figura 13.

Figura 13. Diagrama de Red Sisland Server

Fuente: Innovacion Global

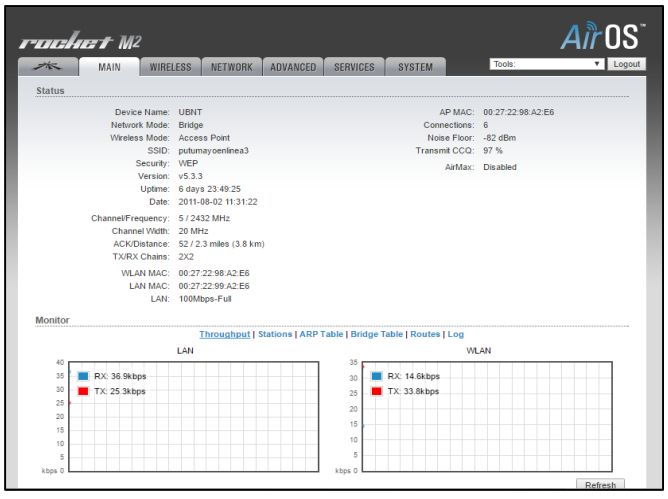
Otro componente a considerar son los puntos de acceso o AP los cuales tienen su firmware interno que permiten su manipulación y control respectivo; se tomara a uno como ejemplo el equipo Ubiquiti rocket M2 ya que son varios puntos de acceso se muestra en la figura 14.

Figura 14. Equipo Ubiquiti Rocket M2

Fuente: http://www.wifi-stock.com/details/ubiquiti_rocketm2.html

El Rocket M2 es un radio de alta potencia con la funcionalidad de receptor mejorado cuenta con un rendimiento aproximado de 50 kilómetros, la velocidad de transferencia de 150 Mbps; este dispositivo ha sido diseñado específicamente para al aire libre con puente punto a punto entre otras, su firmware permite su manipulación y control tal como se muestra en la figura 15.

Figura 15. Firmware Rocket M2



Fuente: Innovación Global

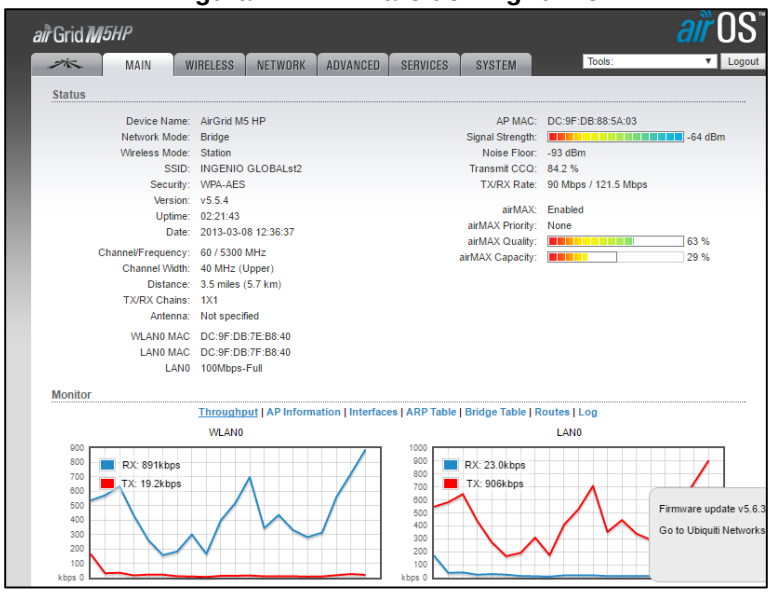
Finalmente se tiene en consideración las estaciones de trabajo las que permiten la conexión de los usuarios a la red de innovación global, son muchas las marcas de equipos que se utilizan por lo tanto se toma una como ejemplo que es el equipo Ubiquiti Airgrid M5, estos dispositivos dependen de la frecuencia que se los utiliza en este caso de 5 Ghz y acorde al AP que está conectado, se muestra en la figura 16.

Figura 16. Ubiquiti Airgrid M5

Fuente: http://www.ubiquiticolombia.com/ubiquiti-airgrid-m5-hp-23dbi/

Ubiquiti Airgrid M5, integra un sistema de radio de antena potente y robusta capaz de traficar 100 Mbps reales de rendimiento al aire libre con un rendimiento de 10 a 15 kilómetros en enlace punto a punto y se muestra su configuración en el firmware en la figura 17.

Figura 17. Firmware de Airgrid M5



Fuente: Innovación Global

7.6 ACTIVOS DE LA RED DE SIBUNDOY DE LA EMPRESA INNOVACIÓN GLOBAL

Los activos de la empresa innovación Global SAS son los siguientes:

HARDWARE

PUNTOS DE ACCESO
1 sectoriales ubiquiti airmax sector am2g16
1 equipo para sectoriales ubiquiti rocket m2
6 ap ubiquiti nanostation m5
1 ubiquiti bullet m2hp
8 antena sectorial de 2.4 ghzdbi, apertura 120 grados polarización vertical
1 antena omnidireccional profesional 2.4 ghz 12 dbi

ESTACIONES DE TRABAJO USUARIO
4 ubiquitiairgrid m2 – hp 20 dbi clientes especiales
15 estaciones clientes ubiquiti nanostation loco m2
Estaciones 40 ubiquiti nanostation loco m5

ENLACES
2 equipos motorolacanopy 10mbps wirelessbackhaul
6 ubiquiti nanobridge m2 18dbi

ENRUTADORES Y CONCENTRADORES
2 mikrotik rb450
3 mikrotik rb750g
4 switch 16 puertos gigabit tp-link 10/100/1000 tl-sg1016d

EQUIPOS
1 portátilToshibaSatellite cl10-b
1 impresora Epson l210
1 impresora lexmark cx510de
1torre alta gama core i7 4770k,r9 295 x2 8gb,evga 1300w.
4 equipos torre cpuintelquadcore q6600\3gb\320g\nvidea 9400gt.

SOFTWARE
- Sisland server 12.12

- Windows 8
- windows 7
- ofimática

COMUNICACIONES
Red inalámbrica
Red Local
Internet
Red telefónica

INSTALACIONES
Casa Familiar de Roberto Vallejo
Edificio Cámara de Comercio de Sibundoy
5 torres de 40 metros cada 1

EQUIPOS AUXILIARES
4 ups
4 estabilizadores de corriente
1 planta eléctrica Yamaha 2600
Herramienta
Mobiliario
Carro Twingo 2010

RECURSO HUMANO. Integrado por personal de Innovación Global y sus usuarios

7.7 REGISTRO FOTOGRÁFICO DE LA INFRAESTRUCTURA TECNOLÓGICA DE INNOVACIÓN GLOBAL SAS

A continuación se indica el registro fotográfico realizado a las áreas donde se ubican los equipos que permiten realizar la conexión y control de la red como la disposición de las antenas donde se ubican los puntos de acceso.

Figura 18. Ubicación del servidor

Fuente: Los autores

Como se puede observar en la Figura 18 el área donde se ubica el servidor y dispositivos necesarios para la conexión esta desordenada.

Figura 19. Estado de las Conexiones

Fuente: los autores

En la Figura 19, se puede observar que no se cuenta con suficientes tomacorrientes regulados, por lo cual ha sido necesario conectar los equipos

directamente a la red de corriente normal, que pone en riesgo los equipos ante fallas por variaciones de voltaje de la red de Innovación Global.

Figura 20. Torre A

Fuente: Los autores. Torre A ubicada en casa del señor Roberto Vallejo Santacruz

Figura 21. Torre B

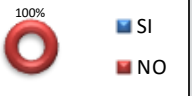
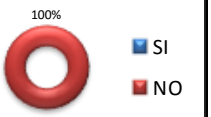
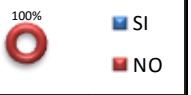
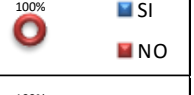
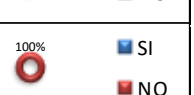
Fuente: los autores.

Torre B. ubicada en el edificio de la cámara de comercio del Valle del Sibundoy Putumayo. Las torres (antenas) A y B tienen puntos de acceso con frecuencia de 2.4 GHZ y 5.4GHZ

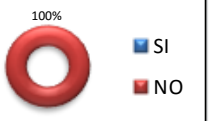
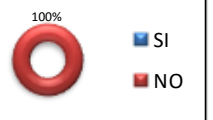
7.8 ENTREVISTA

La entrevista se realizó al administrador de la red, y los 2 técnicos. La entrevista se realizó con el fin de determinar los mecanismos de seguridad que disponen en el momento. El cuestionario involucro 20 preguntas de tipo cerrado. En la tabla 3 se indican las respuestas obtenidas por el personal entrevistado. Tabla 3. El formato del cuestionario de la entrevista se presenta en el anexo B.

Tabla 3. Resultados de la entrevista

ITEMS	Adm. Red		Técn. 1		Técn. 2		RESULTADOS		Tabulacion Gráfica
	Si	No	Si	No	Si	No	SI	NO	
ESTRUCTURA ORGANIZACIONAL									
1. ¿Se cuenta con una estructura organizacional de apoyo para la seguridad de la red y la información?		x		x		x	0	3	
2. ¿Se ha contado con algún tipo de auditoria que verifique el buen funcionamiento del sistema informático de la empresa?		x		x		x	0	3	
POLÍTICAS Y NORMAS DE SEGURIDAD									
3. ¿Se cuenta con políticas, normas y procedimientos establecidos para mejorar la seguridad de la red y la protección de la información?		x		x		x	0	3	
PLANES DE SEGURIDAD									
4. ¿Existen planes y programas o procedimientos de seguridad actualizados para garantizar el funcionamiento normal de la red en caso de: incendios, fallas eléctricas, inundaciones, ataques al sistema de información de la empresa, entre otros?		x		x		x	0	3	
AMENAZAS Y VULNERABILIDADES									
5. Existen planes para prevenir ataques a corto y largo plazo debido a vulnerabilidades posibles en la red física y lógica de la empresa?		x		x		x	0	3	
GESTIÓN DE USUARIOS									
6. ¿Se tiene un registro de las transacciones realizadas por los usuarios del sistema?		x		x		x	0	3	
7. ¿Se cuenta con normas o políticas escrita acerca del uso y responsabilidades de las contraseñas?		x		x		x	0	3	
8. ¿Existe un registro de los eventos o incidentes que pueden afectar la seguridad de la red y los datos?		x		x		x	0	3	
9. ¿Se realiza un análisis del tráfico de la red para determinar posibles instrucciones o identificar protocolos que circulen en ella?		x		x		x	0	3	
10. ¿Se cuenta con un sistema de control de intrusos o IDS?		x		x		x	0	3	

Continuación tabla 3. Resultados de la entrevista

ITEMS	Adm. Red		Técn. 1		Técn. 2		RESULTADOS		Tabulacion Gráfica
	Si	No	Si	No	Si	No	Si	No	
CÓDIGO MALICIOSO O VIRUS									
11. ¿se tiene controles para impedir la propagación de virus y código malicioso, son esporádicos o periódicos?		x		x		x	0	3	
CONTINUIDAD									
12. ¿Se efectúan mediciones periódicas del desempeño, capacidad o calidad del servicio de la red?	x		x		x		3	0	
UMBRALES DE SERVICIO									
13. ¿Se conoce en detalle los niveles aceptables de tráfico del servicio de la red para determinar los valores normales del tráfico definido?		x		x		x	0	3	
PLANES DE CONTINUIDAD									
14. ¿Existen planes o servicios que describan los procedimientos para recuperar y reanudar el servicio ocasionado por algún incidente en la red que permiten garantizar la continuidad del servicio de la red y sus datos?		x		x		x	0	3	
SOPORTE DE TERCERAS PARTES EN LOS PROCESOS DE CONTINGENCIA Y RECUPERACIÓN									
15. ¿Se tiene algún tipo de contrato con otra empresa para soporte para solventar problemas respecto a la continuidad de operaciones?		x		x		x	0	3	
SEGURIDAD EN LAS REDES DE DATOS									
16. ¿La arquitectura de la red está debidamente documentada?		x		x		x	0	3	
17. ¿Todos los equipos de la red están debidamente identificados y lugar de ubicación es adecuado para los mismos?	x		x		x		3	0	
POLÍTICAS Y NORMAS									
18. ¿Se tiene por escrito las normas que regulan la disposición del cableado de red y de la energía eléctrica?		x		x		x	0	3	
SEGURIDAD FÍSICA									
19. ¿Se tienen políticas escritas y claras que orienten el acceso físico a la infraestructura de la red, servicios de Internet por parte de los usuarios del sistema?		x		x		x	0	3	
20. ¿Se ofrecen capacitaciones al personal a cargo de la red que favorezca la seguridad y buen funcionamiento de la red y lo que esta concierne?		x		x		x	0	3	

Fuente: los autores

8. IDENTIFICACIÓN DE VULNERABILIDADES Y AMENAZAS

En este capítulo se tiene en cuenta lo evidenciado en el registro fotográfico realizado en la empresa, los resultados de la entrevista, observación directa. Así mismo se indican los resultados de las pruebas de pentesting realizadas. Completando este capítulo finalmente, se presenta la valoración de las vulnerabilidades y amenazas en los activos informáticos teniendo en cuenta la metodología de MAGERIT.

8.1 ANÁLISIS DE RESULTADOS PRELIMINARES

Para verificar el estado físico de los bienes que soportan la operatividad de la red informática de Innovación Global, se realizó el registro fotográfico del sitio donde se ubica el servidor y sus respectivas instalaciones. Los resultados fueron los siguientes:

8.1.1 Ubicación de equipos y estructura lógica de la red

De acuerdo al registro fotográfico como la observación y charlas informales con personal de la empresa se encontró lo siguiente:

- Las estaciones de trabajo, no cuenta con condiciones necesarias para un eficiente funcionamiento
- Hay equipos de red que no cuenta con un debido regulador de voltaje.
- En cuanto a las claves de acceso, tanto a las estaciones de trabajo como a los puntos de acceso, no se cambia con frecuencia
- No se cuenta con un sistema de pararrayos
- No se cuenta con un suministro de energía alterno,
- Las frecuencias de 2.4 Ghz presentan fallas de ruido y latencia
- No se cuenta con un cuarto de comunicaciones y de energía adecuado
- El sitio donde se ubica el servidor y otros equipos de interés para el funcionamiento de la red, no cuenta con ventilación adecuada. Se observa acumulación de polvo en su entorno, por lo cual es probable que también

en el interior de los equipos exista polvo que puede sobrecalentar los circuitos y dañar en los dispositivos internos. Además se observa que los cables están desorganizados, y hay elementos que no corresponden a esta área.

- No existe un tablero regulado con disyuntores automáticos que permitan controlar un determinado estado (circuito abierto, apagado).

- Los tomacorrientes de voltaje regulado no cuentan especificaciones técnicas.

- No existe un cableado estructurado de todos los equipos inalámbricos y dispositivos, tampoco cuentan con una identificación adecuada

- la red no está normalizada ni documentada debidamente.

- En las antenas se observa un desgaste de los equipos inalámbricos. Y presentan una congestión en el espectro debido a que se tiene varias redes inalámbricas.

8.1.2 Conclusiones de la entrevista realizada

De acuerdo a la tabulación de las respuestas obtenidas en la entrevista al administrador de la red y a los dos técnicos se tienen las siguientes conclusiones:

- Los resultados obtenidos respecto al marco organizacional requerido para dar respaldo a las actividades de seguridad, indican que no se cuenta con un departamento de seguridad de la información y no se ha realizado una auditoría de sistemas. Así se observa que la empresa de Innovación Global no cuenta con las políticas, normas y procedimientos documentados y definidos claramente que regulen lo referente la seguridad de la información de la empresa.

- Con respecto a las amenazas que pueden presentarse, la empresa no cuenta con un plan que permita afrontar eventuales incidentes que pueden afectar el sistema informático de la empresa. igualmente no se tienen planes que permitan realizar una labor preventiva respecto a las vulnerabilidades de los sistemas y de las redes de datos.

- Respecto a la continuidad del servicio, se puede decir que no está garantizada, debido a que no se realizan mediciones de la capacidad actual, por lo que no se puede predecir una futura saturación de la red misma. Así mismo se carece de planes y programas de continuidad del servicio. No se tiene contratos de mantenimiento con terceros.

- En cuanto a la gestión de usuarios, existen algunas deficiencias, debido a que no se cuenta con los registros adecuados que permitan ejecutar procesos de revisión; no se regula adecuadamente el proceso de otorgamiento de privilegios, así como tampoco existen las políticas y normas relativas a las responsabilidades de los usuarios y sus contraseñas en el sistema.

- Con respecto a los códigos maliciosos, no se tienen controles eficientes que impidan su propagación en la red.

- La falta de unas políticas y normas de seguridad afecta la seguridad física, y lógica de la red, pese a ello el personal a cargo de la red trabajan para restringir el acceso de personas no autorizadas a las instalaciones como a la red en sí.

8.1.3 Pruebas de Pentesting

Las pruebas de penetración (también llamadas “pen testing”) son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar[23]

Con el fin de determinar las debilidades de seguridad de la red de Innovación Global, se realizaron pruebas mediante las aplicaciones de Nmap y OWASP ZAP, DDos Attack: Slowloris, Unknown DoSer release, Aircrack-ng, Wifite;las. Las pruebas se realizan con el permiso del gerente de la empresa y de acuerdo a lo dispuesto en los artículos de la ley 1273 del 2009.[24]

[23] http://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

[24] Ley 1273 de 2009, hace referencia a la protección de la información y de los datos, por lo cual el uso de aplicaciones para determinar las debilidades de la red se realiza de forma controlada de tal forma que no perjudique la integridad de la información de la empresa en ningún sentido.

Teniendo en cuenta la estructura de la red inalámbrica de innovación global se especifica cuatro ataques generales así:

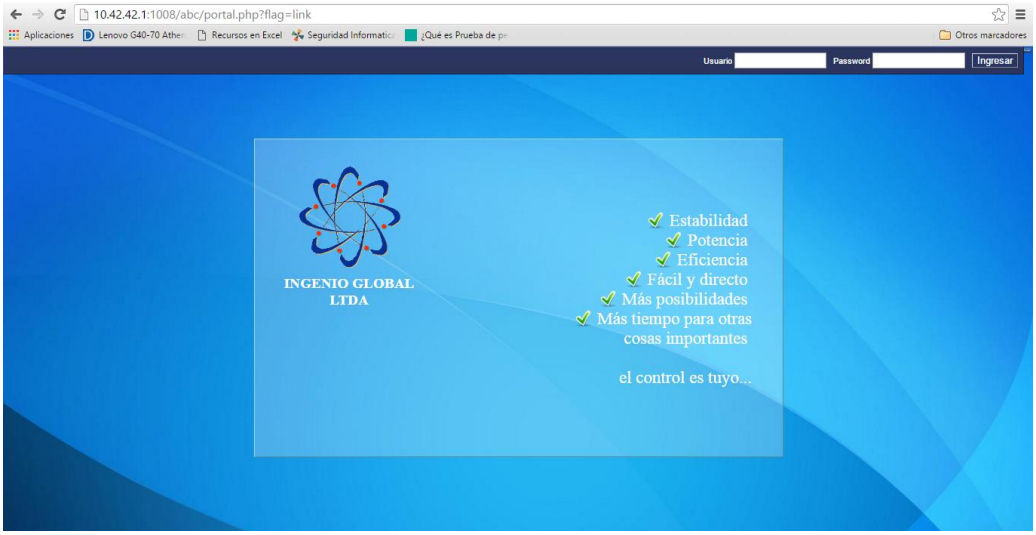
8.1.3.1 Denegación del Servicio

Estos ataques son los más difícilmente evitables puesto a cómo funcionan las tecnologías inalámbricas ya que alguien puede generar suficiente ruido y hará imposible la comunicación entre los dispositivos afectando la disponibilidad de la red.[25]

Para esta prueba se selecciona el servidor sisland server el cual es el que gestiona el tráfico de la red y considera de bastante prioridad para la empresa.

Su dirección para el ingreso respectivo es:
http://10.42.42.1:1008/abc/portal.php?flag=link

Figura 22. Interfaz Sisland server

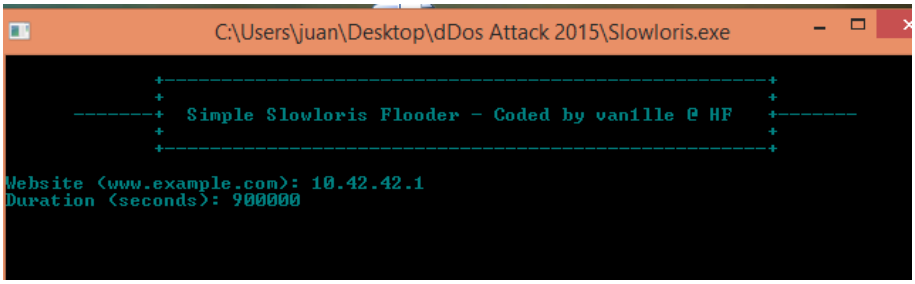


Fuente: innovación global

Se utiliza dos aplicaciones para la denegación del servicio DDos Attack: Slowloris, Unknown DoSer release[26]

[25] Video lección 12: seguridad en redes Wi-Fi(intypedia)
[26] http://www.eticalhacking.com.mx/descargas/

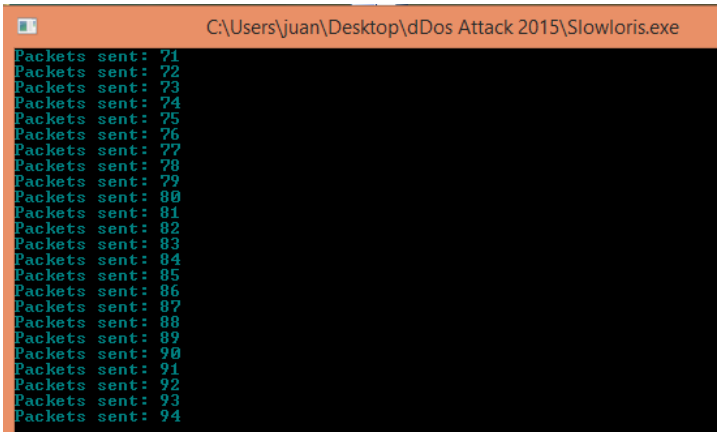
Figura 23. Aplicación Slowloris



Fuente: los autores

La configuración de esta herramienta es colocar la ip del servidor que corresponde 10.42.42.1 y su duración en segundos es 900000, al dar enter se obtiene un sin número de peticiones como se observa en la Figura 23

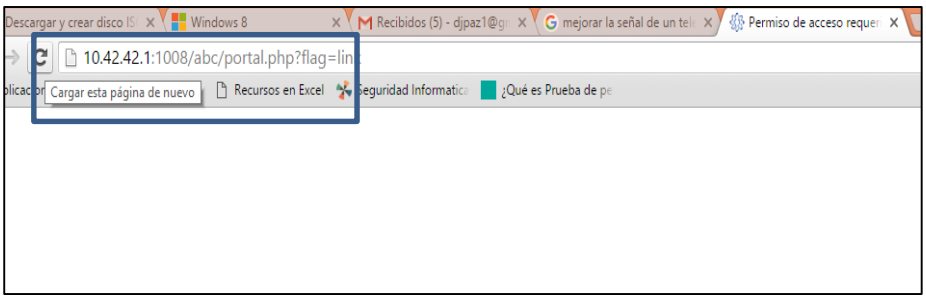
Figura 24. Funcionamiento de Slowloris



Fuente: los autores

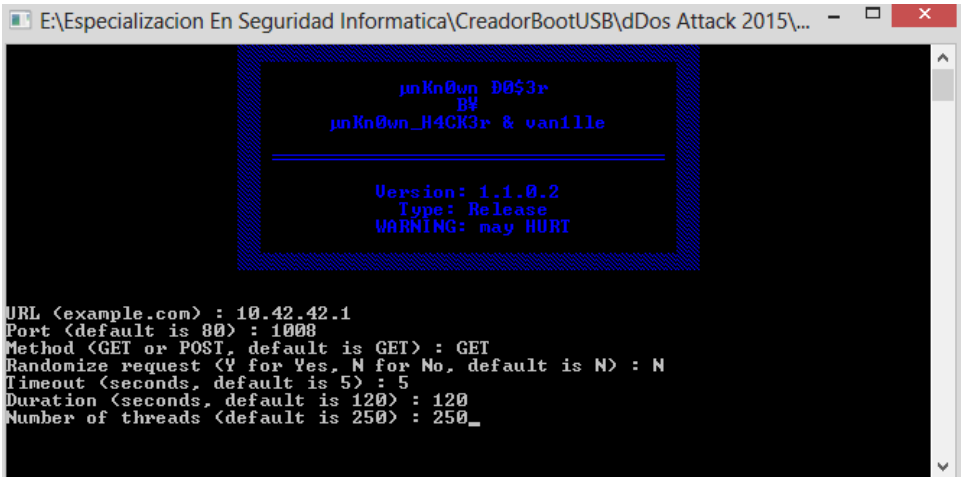
El objetivo de este ataque es enviar paquetes para colapsar el servidor tal como se muestra en figura 24. En la figura 25 se puede observar la caída de la señal de internet debido al envío de paquetes.

Figura 25. Denegación de servicio con Slowloris



Fuente: los autores

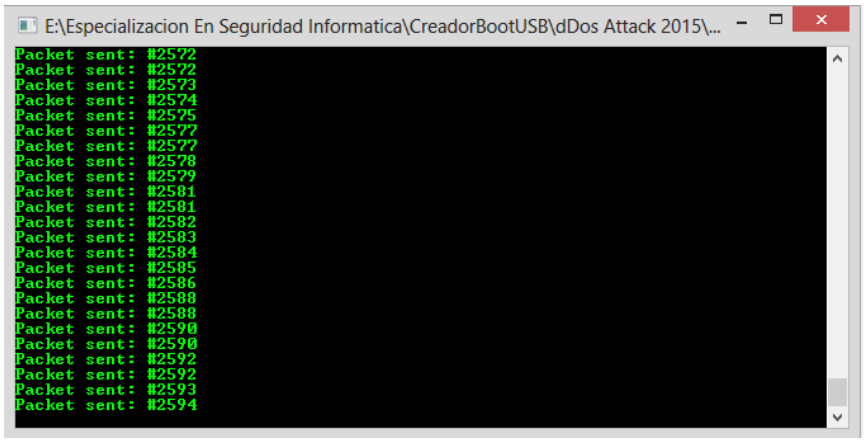
Figura 26. Aplicación Unknown DoSer reléase



Fuente: los autores

La configuración de esta herramienta es colocar la ip del servidor 10.42.42.1 y el puerto de acceso 1008, el método get y su lapso de tiempo en milisegundos 5,120, 250(figura 26), para que al dar enter se obtenga un sin número de paquetes enviados tal como lo muestra la figura 27.

Figura 27. Funcionamiento Unknown DoSer reléase



Fuente: los autores

La consecuencia de los paquetes enviados es saturar la interfaz del servidor y no permitir su ingreso obteniendo la denegación de este servicio el cual proporciona la manipulación del servidor. Figura 28

Figura 28. Denegación del servicio Unknown DoSer reléase

Fuente: los autores

8.1.3.2 Interceptar datos de la Red

Este ataque consiste en interceptar las comunicaciones que viajan por el aire modificando su contenido y afectado su integridad, se considera indetectable. A continuación se indican ataques realizados al servidor mediante Nmap

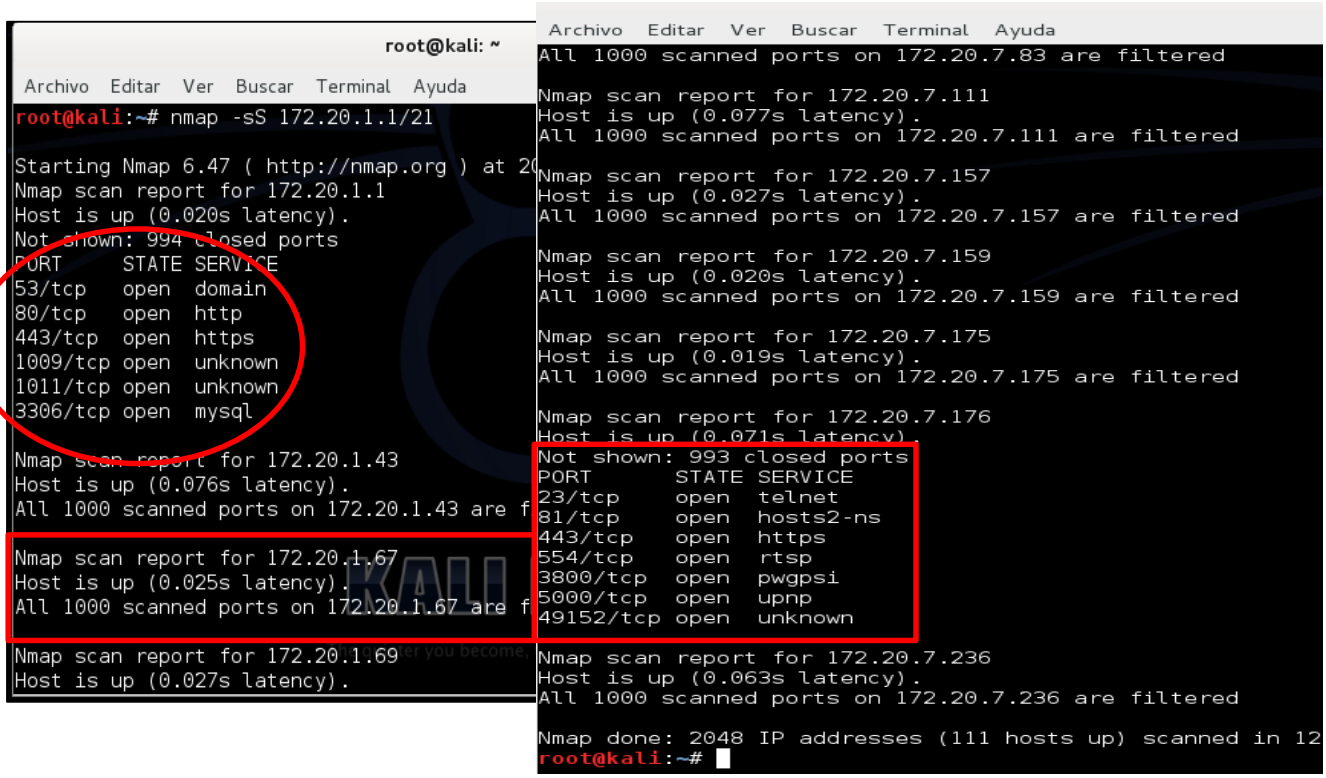
Nmap ("mapeador de redes"). Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.[27]

Teniendo en cuenta la infraestructura de red inalámbrica por parte de la empresa Innovación Global se considera la utilización de herramientas de explotación de vulnerabilidades por medio de un sniffing, en éste caso se realizan pruebas con Nmap, para determinar que puertos están abiertos dentro de la red y así detectar posibles fallas del sistema de seguridad.

Mediante el comando –sS, que es un sondeo TCP SYN medio abierto, se sondea los puertos en la que no existen firewalls tal como se observan en la figura 29.

[27] https://nmap.org/man/es/

Figura 29. Uso de comando nmap comando –sS

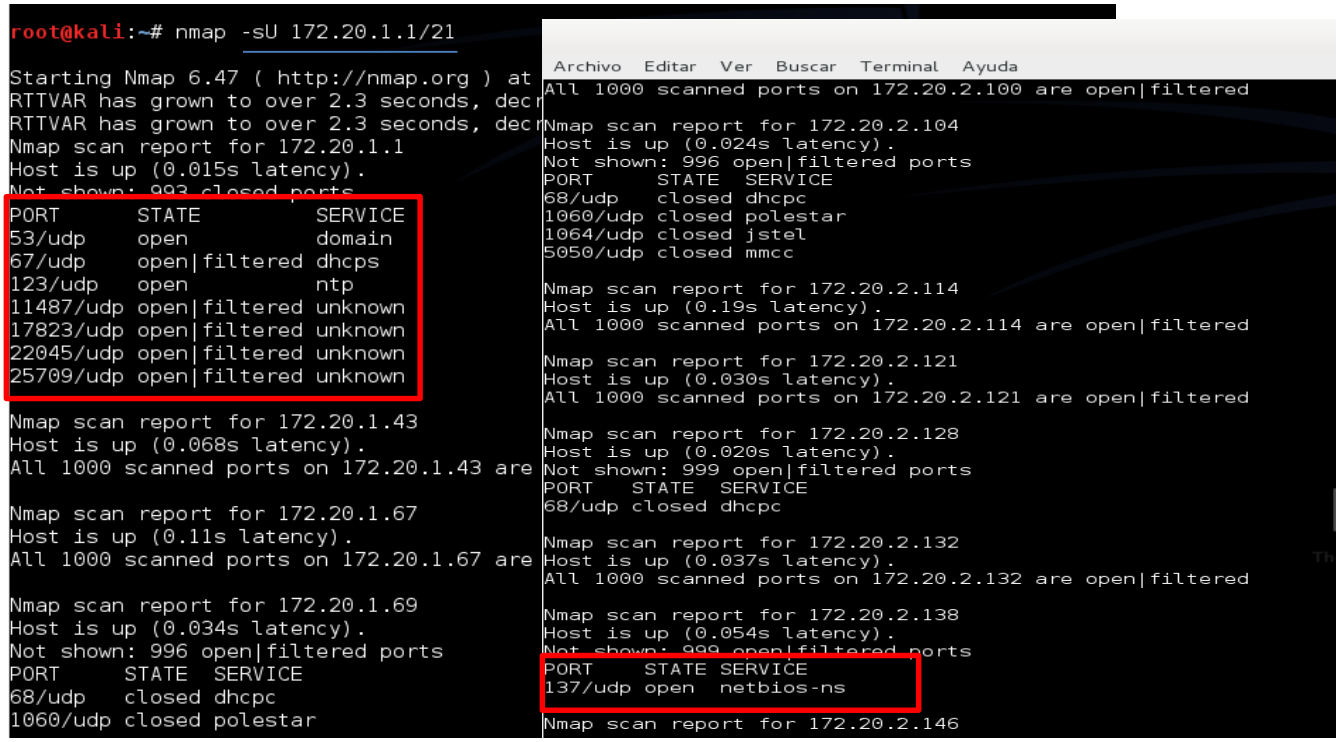


Fuente: Los autores

El resultado del comando se interpreta de la siguiente manera: nmap –sS 172.20.1.1/24 corresponde a la red general de la empresa. Como se observa se visualizan algunos puertos abiertos en este caso es el servidor.

Con este de sondeo de puertos se determinan también que terminales de los clientes tienen puertos abiertos.

Figura 30. Sondeo UDP

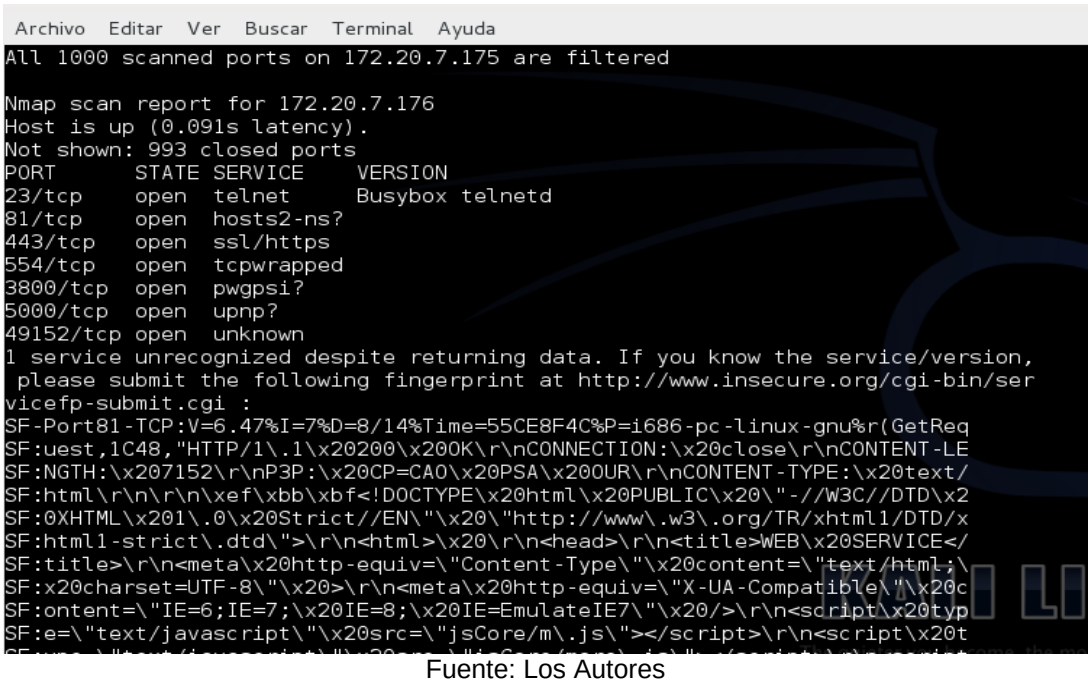


Fuente: Los Autores

Mediante el comado –sU, se realiza un sondeo UDP, ya que son servicios vulnerables que por lo general no son protocolos ignorados por los atacantes; el sondeo UDP se puede combinar con un tipo de sondeo TCP como el sondeo SYN, así es posible comprobar ambos protocolos al mismo tiempo. En la figura 30, se indica el resultado de ejecutar el comando –sU.

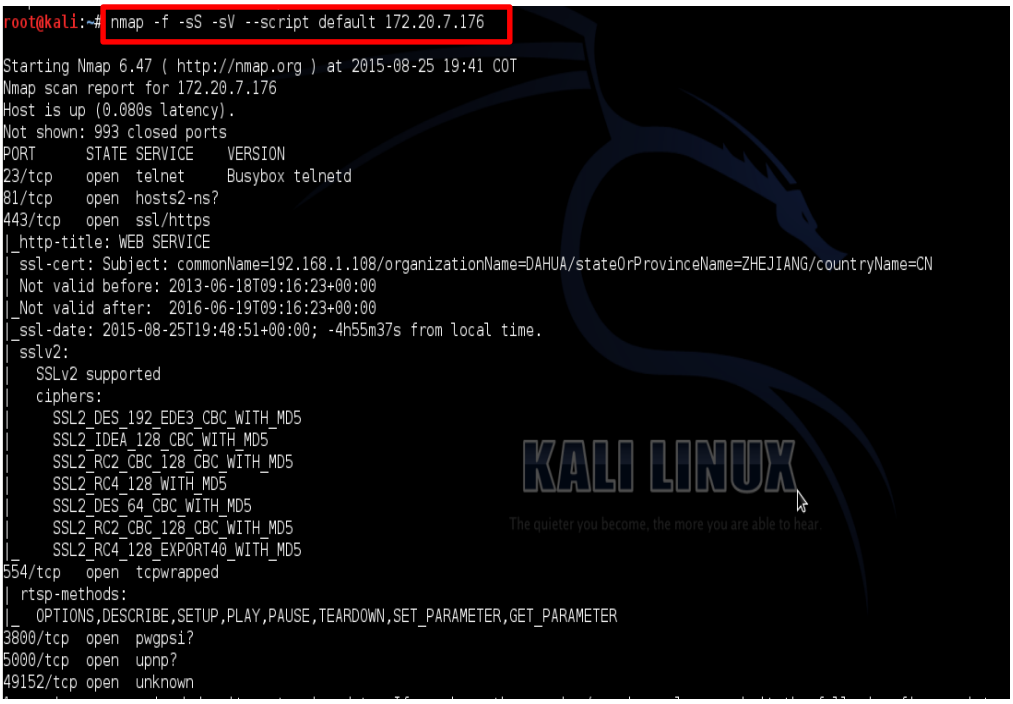
Una vez detectado los puertos que están abiertos, mediante el comando -sV el cual permite la detección del sistema operativo, se procede a conocer cuáles son las máquinas que los generan como se indica en la figura 31.

Figura 31. Resultado de ejecutar el comando -sV



Fuente: Los Autores

Figura 32. Ejecución de la línea de comando nmap -f -sS -sV -script



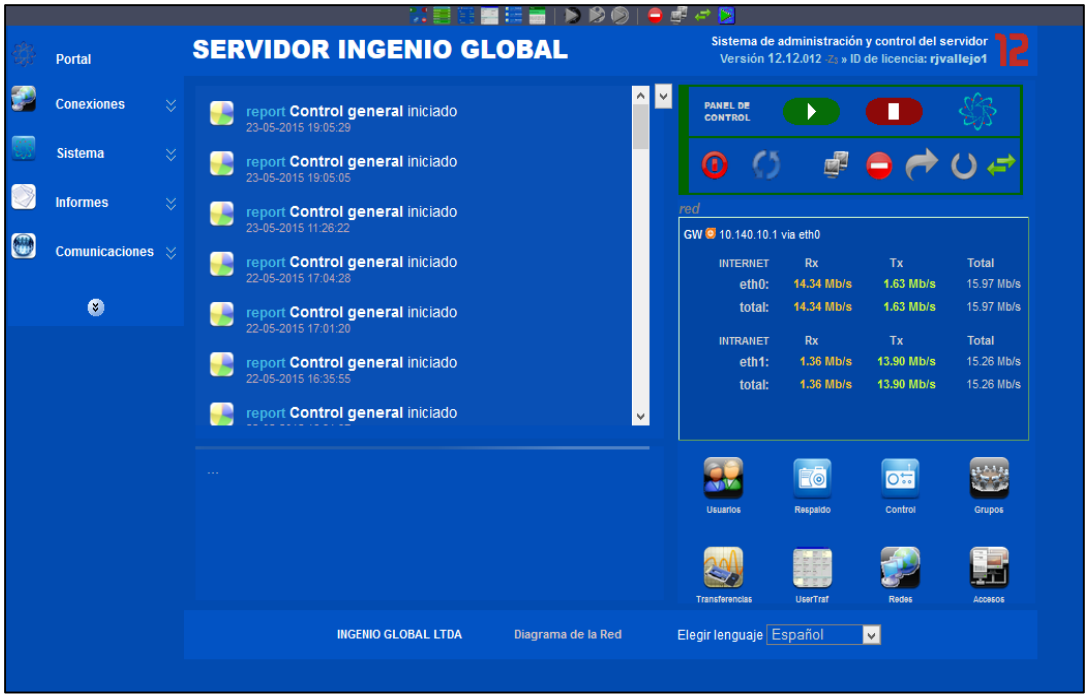
En la figura 32, se indica un ataque específico a un cliente o usuario con fin de determinar su sistema operativo y aplicar un método de metaexploit al puerto abierto para ello se utiliza el comando nmap -f -sS -sV –script

Con esta práctica se pretende hacer un diagnóstico de la red inalámbrica en la cual se identifican a clientes o usuarios que presentan deficiencias en cuanto a puertos específicos susceptibles a ataques de metaexploit, manipulación y pérdida de información confidencial.

8.1.3.3 Pruebas con OWASP ZAP

La realización de esta prueba es para el servidor principal de la empresa Innovación Global, en este caso es Sisland Server 12.12, el cual permite la administración del canal de internet como el registro de los usuarios y sus movimientos en la red. En la figura 14 se muestra en entorno grafico del servidor.

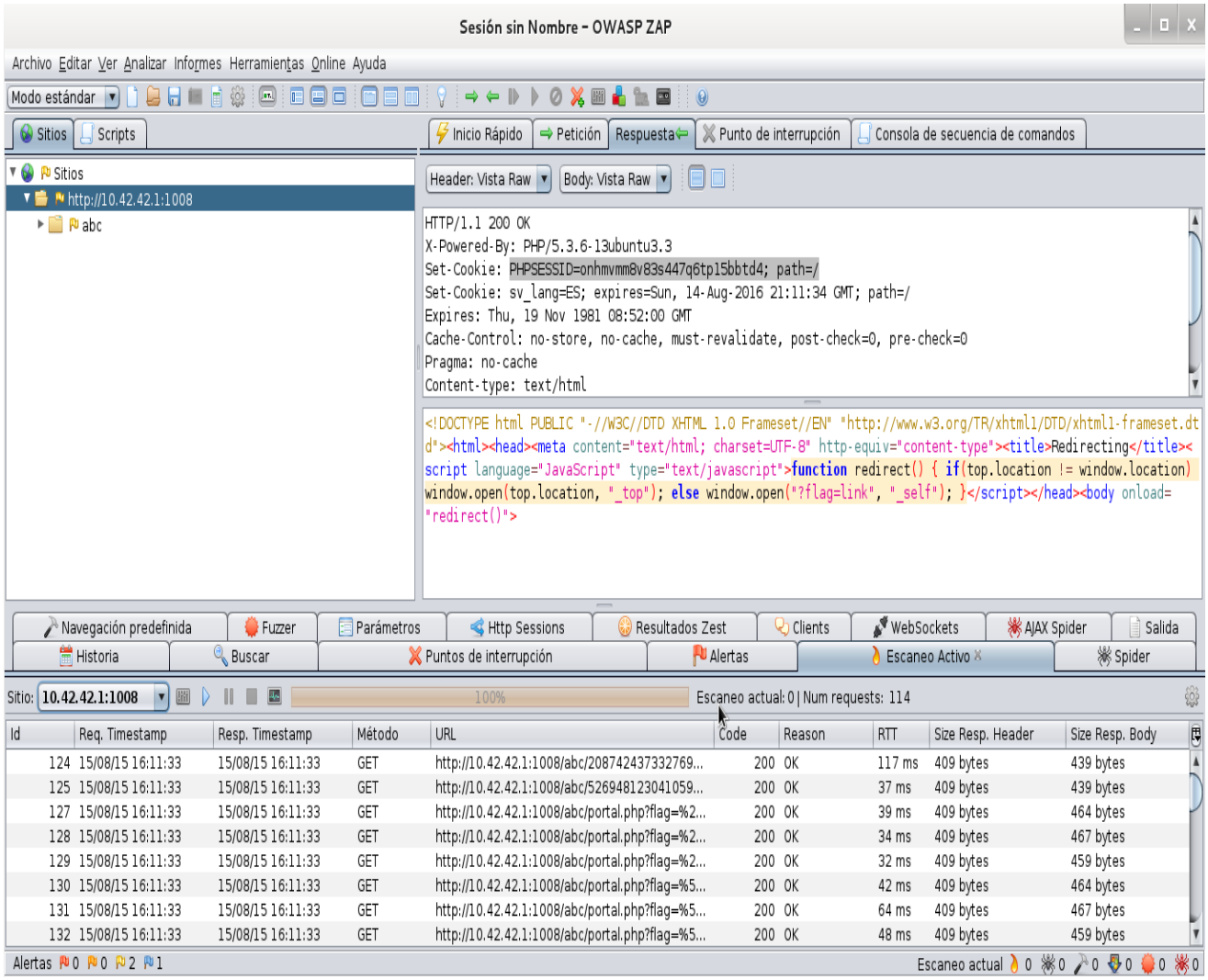
Figura 33. Servidor sisland server 12.12



Fuente: Los Autores

El ingreso a este entorno grafico del servidor puede hacerse desde cualquier parte siempre y cuando se tenga acceso a internet y tener presente la Ip publica del proveedor de Innovación Global y desde la red inalámbrica con la siguiente IP 10.42.42.1 puerto 1008, el cual va ser sometido a esta pruebas con OWASP ZAP y con el consentimiento de la empresa. Fig. 33

Figura 34. Ejecución de OWASP ZAP

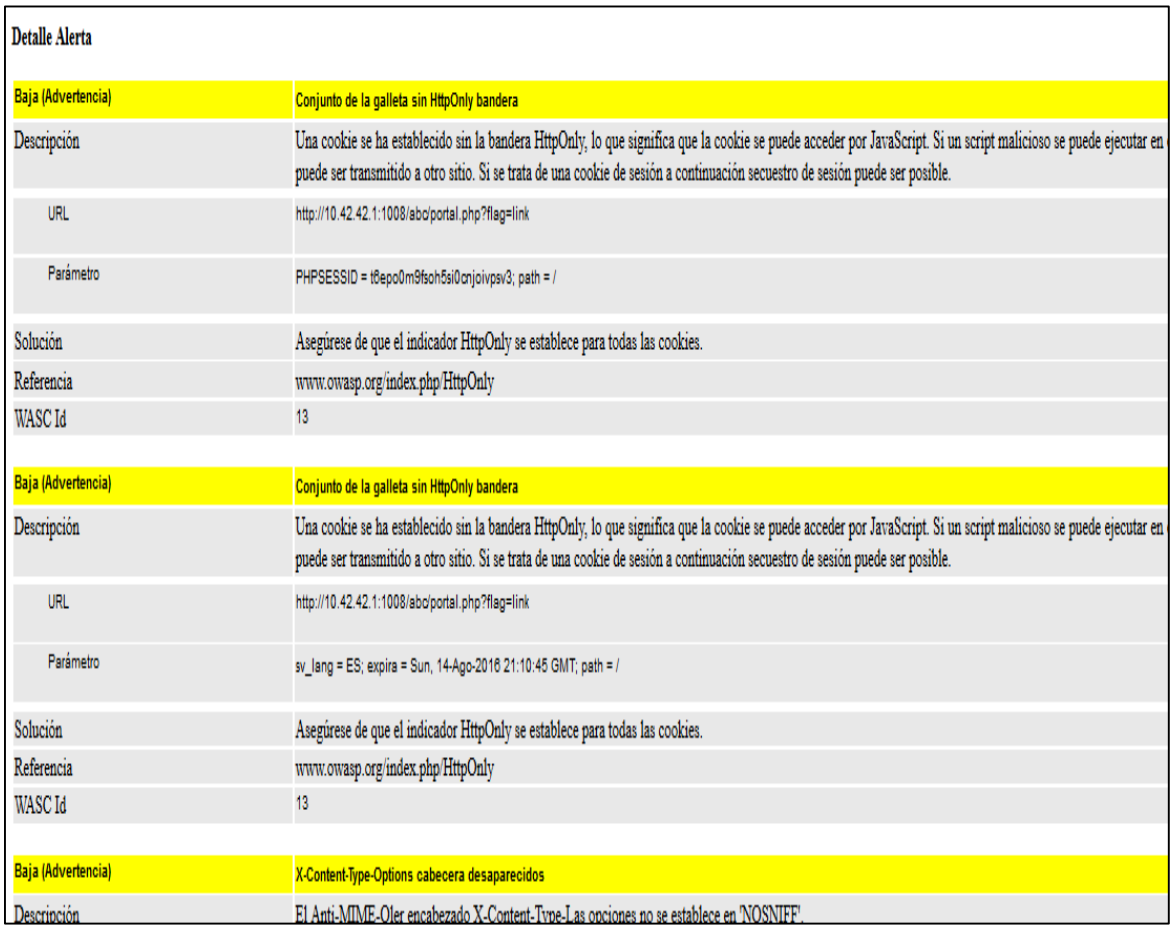


.

Fuente: Los Autores

Esta herramienta permite generar un reporte en html en donde se ven las deficiencias y posibles soluciones; en este caso se detectaron 8 vulnerabilidades en término bajo y 1 un informativo, los cuales afirman que el servidor cuenta con una seguridad que puede ser tolerada, pero podemos que puede ser mejorada como se observa en la figura 35

Figura 35 Reporte generado en html



Detalle Alerta	
Baja (Advertencia)	Conjunto de la galleta sin HttpOnly bandera
Descripción	Una cookie se ha establecido sin la bandera HttpOnly, lo que significa que la cookie se puede acceder por JavaScript. Si un script malicioso se puede ejecutar en puede ser transmitido a otro sitio. Si se trata de una cookie de sesión a continuación secuestro de sesión puede ser posible.
URL	http://10.42.42.1:1008/abc/portal.php?flag=link
Parámetro	PHPSESSID = t8epo0m9fsoh5si0cnjoivpsv3; path = /
Solución	Asegúrese de que el indicador HttpOnly se establece para todas las cookies.
Referencia	www.owasp.org/index.php/HttpOnly
WASC Id	13
Baja (Advertencia)	Conjunto de la galleta sin HttpOnly bandera
Descripción	Una cookie se ha establecido sin la bandera HttpOnly, lo que significa que la cookie se puede acceder por JavaScript. Si un script malicioso se puede ejecutar en puede ser transmitido a otro sitio. Si se trata de una cookie de sesión a continuación secuestro de sesión puede ser posible.
URL	http://10.42.42.1:1008/abc/portal.php?flag=link
Parámetro	sv_lang = ES; expira = Sun, 14-Ago-2016 21:10:45 GMT; path = /
Solución	Asegúrese de que el indicador HttpOnly se establece para todas las cookies.
Referencia	www.owasp.org/index.php/HttpOnly
WASC Id	13
Baja (Advertencia)	X-Content-Type-Options cabecera desaparecidos
Descripción	El Anti-MIME-Oler encabezado X-Content-Type-Las opciones no se establece en 'NOSNIFF'.

Fuente: Los Autores

8.2 VALORACIÓN DE VULNERABILIDADES Y AMENAZAS EN LOS ACTIVOS INFORMÁTICOS

En esta sección se realiza la valoración de vulnerabilidades y amenazas en los activos informáticos teniendo en cuenta la metodología de MAGERIT V3. Mediante esta metodología se realizara el análisis de riesgos con el fin de determinar las medidas de control adecuadas que se pueden implementar para mitigar los riesgos asociados a vulnerabilidades encontradas en la empresa de Innovación Global, en cuanto a su red inalámbrica; que le permitirán posteriormente adoptar medidas para identificar, prevenir y controlar los riesgos encontrados y que reduzcan al máximo sus perjuicios. Esta metodología, está alineada con los estándares de la norma ISO, lo cual permitirá, diseñar el SGSI, acorde a las necesidades de Innovación Global.

8.2.1 Caracterización y Valoración de los Activos

En este punto se tiene en cuenta la identificación y valoración de activos

8.2.1.1 Identificación de activos

De acuerdo a MAGERIT, para diferenciar los activos es necesario agruparlos en varios tipos según la función que ejerzan en el tratamiento de la información. Los activos según MAGERIT se agrupan en activos relevantes que están subordinados a los activos esenciales de toda empresa como son los servicios y la información; estos grupos de activos son: [28]

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos
- Los equipos informáticos (hardware) y que permiten hospedar 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.

[28] Activos. Recuperado de: Magerit_v3_libro1_método_es_NIPO_630-12-171-8%20(10).pdf

- Las personas que explotan u operan todos los elementos anteriormente citados.

En la tabla 4 se relacionan los activos de seguridad de la información de la empresa Innovación Global, que se relacionan con su red inalámbrica.

Tabla 4. Relación de activos para la red inalámbrica de Innovación Global

Grupos de activos y nomenclatura según Magerit	Código y nombre del Subgrupo del activo según Magerit	Código de identificación y nombre del activo correspondiente a cada grupo
[info]información: **Activos esenciales**	**[Vr].** Datos vitales (registros de la empresa)	**[Vr].** Bases de datos control de usuarios y pagos. **[Vr].** Información de licencias **[Vr].** Información de Normativa (Normas locales, nacionales, acuerdos, decretos)
	[Per]. Datos de Carácter personal	**[Per].**Contabilidad de la empresa
	[Classified]. Datos clasificados	**[Classified].**Ejecutable software Licenciador
[info]información: **[D] Datos/ información**	**[Files].** Ficheros	**[Files].** Contratos de afiliación de usuarios y del personal que labora en Innovación Global **[Files].** Matricula de telecomunicaciones para el funcionamiento de Innovación Global
	[backup]. Copias de respaldo	**[backup].** Copias de respaldo y datos de configuración del servidor y de las estaciones de trabajo y puntos de acceso.
	[Conf]. Datos de configuración	**[Conf].** Datos de configuración del servidor y equipos
	[Password]. Credenciales	**[Password].** Contraseñas de acceso de empleados
	[Log]. Registro de actividad	**[Log][29].** Registros de archivos logs
	[acl] datos de control	**[acl]** datos de control de Acceso

[29] **Logs.** Son ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste. http://www.alegsa.com.ar/Dic/log%20de%20servidor.php

Grupos de activos y nomenclatura según Magerit	Código y nombre del Subgrupo del activo según Magerit	Código de identificación y nombre del activo correspondiente a cada grupo
[keys] Claves criptográficas	**[encrypt]** claves de cifra	**[encrypt].** Claves de los APS
[S] Servicios	**[ext].** a usuarios externos (bajo una relación contractual) **[int].** interno (a usuarios de la propia organización)	**[ext] .** Conectividad a internet y soporte técnico para usuarios externos **[int].** Servicio de internet para usuarios internos
[SW] Software de aplicación	**[os].** Sistema operativo **[office]**.Ofimática **[av]**. Anti virus	**[os].** Sisland Server 12.12. Software para controlar y optimizar el servicio de internet en toda la red. **[so].**Windows 8 en equipos de soporte **[so].**Windows 7 en equipo de soporte **[office]**. Aplicaciones Ofimáticas. office 2010 **[av].** Antivirus Norton en equipos de soporte con LC.
HW] Equipos informático s (hardware)	**[network]** soporte de la red	**[Network].** Dispositivos para el funcionamiento de la red inalámbrica: Antena 1. Ubiquiti Airmax Sector AM2G16 Antena 2 Sectorial de 2.4 GHZ DBI Antena 3 Omnidireccional Profesional 2.4 GHZ Dispositivo inalámbrico Ubiquiti Rocket M2 Dispositivo Inalámbrico Ubiquiti Nanostation M5 Dispositivo Inalámbrico Ubiquiti Nanostation M5 Dispositivo Inalámbrico Ubiquiti Bullet M2hp Dispositivo Inalámbrico Ubiquiti Airgrid M2 – HP 20 DBI Dispositivo inalámbrico Ubiquiti Nanostation Loco M2 Dispositivo inalámbrico Equipos Motorola Canopy 10MBPS WirelessbackhauL Dispositivo Inalámbrico Ubiquiti Nanobridge M2 Dispositivo de red RB/450G MIKROTIK 450G -LAN ports: 5 Dispositivo de red RB/450G MIKROTIK 750G -LAN ports: 5 Dispositivo de red Switch 16 Puertos GigabiT TP-LINK 10/100/1000 TL-SG1016D)
	[host] grandes equipos. **[mobile].** informática móvil **[pc]** informática personal **[IMP].** Medios de Impresión	**[Host- servidor ISP].** Computador Intel Dual Core 7 con S.O Sisland Server. **[mobile].** Portátil Satellite CL10-B-100.S.O Win8 **[PC].** Computador Intel Dual Core. S.0 win7 **[IMP].** Impresora Epson **[IMP].**Impresora lexmark

Continuación de la Tabla 5. Relación de activos para la red inalámbrica de Innovación Global

Grupos de activos y nomenclatura según Magerit	Código y nombre del Subgrupo del activo según Magerit	Código de identificación y nombre del activo correspondiente a cada grupo
[COM] Redes de comunicaciones	**[wifi].** red inalámbrica	Red inalámbrica de Innovación Global
	[LAN]. red local	Red Local
	[Internet]. Internet	Internet
	[mobile]. telefonía móvil	Telefonía móvil
[Media] Soportes de información	**Soportes electrónicos** [electronic]	**[disk].** Unidades de backup de configuraciones de equipamiento inalámbrico, discriminado por carpetas.
	.[disk] discos duros	**[disk]** . Backup del servidor
		[disk] . Backup de la BD usuarios externos
	Soportes no electrónicos [non_electronic]	**[printed].** AZ- con los contratos de los usuarios
	. [**printed]** material impreso	**[printed].** AZ- con facturas, soportes contabilidad y licencias
		[printed]. Carpetas Varios
[AUX]Equipamiento auxiliar	**[ups]** sistemas de alimentación ininterrumpida	**[ups]** .Ups del servidor, y computadores de soporte
	[furniture] mobiliario:	**[furniture].** Estantes, armarios, escritorios, archivadores, etc
	Cableado**[cabling]**: **.[wire]** cable eléctrico **.[fiber]** fibra óptica	**.[wire]** cable de la instalación eléctrica **.[fiber]** Cableado estructurado
	[power] fuentes de alimentación	Estabilizadores, Fuentes de poder de los equipos de computo
	[ac] generadores eléctricos	Planta eléctrica de 1200 W

Continuación de la Tabla 6. Relación de activos para la red inalámbrica de Innovación Global

Grupos de activos y nomenclatura según Magerit	Código y nombre del Subgrupo del activo según Magerit	Código de identificación y nombre del activo correspondiente a cada grupo
[L] Instalación	**[building].** Edificio **[mobile].p**lataformas móviles **[car]**	**[building].** Infraestructura donde se localizan los sistemas de información y comunicación, está ubicada en la casa de habitación del señor xx en Sibundoy Putumayo. **[car]** vehículo utilizado para transportar al personal de mantenimiento e instalación de la red.
[P] Personal	**[ui].** usuarios internos **[adm].** administradores de sistemas **[ue]**. usuarios externos	**[ui].** Personal de recepción, área técnica, administrativa y archivo **[adm].** Administrador de sistemas. **[ue]**. Usuarios que acceden al servicio de internet que provee la empresa

Fuente: esta información

Las características propias de los equipos (hardware) se describen en el anexo D.

8.2.1.2 Valoración de activos

Debido a que cada activo cumple una función en la generación, almacenaje o procesamiento de la información su valoración es diferente. De acuerdo a la metodología de MAGERIT Versión 3 para realizar esta valoración de activos se deben tener en cuenta las dimensiones de Valoración**,** las cuales se determinan como las características y atributos que hacen valioso un activo. Los activos se deben valorar de acuerdo a las siguientes dimensiones de seguridad[30]:

[30] Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I Método. Página. 25. Ministerio de Hacienda y Administraciones Públicas. España.

Disponibilidad [D]. Disposición de los servicios a ser usados cuando sea necesario y sin interrupciones para que no afecten la productividad de la empresa.

Integridad [I]. Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

Confidencialidad [C]. Consiste en que la información únicamente sea tratada por personal autorizado evitando así accesos no autorizados que conlleven a la perdida de la confidencialidad de la información de una empresa. Esta valoración es típica de datos

Autenticidad. Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

Trazabilidad [T]. Se refiere a saber quién acceso a los datos y que se hace con ellos.

8.2.2 Criterios de Valoración

Una vez agrupados y clasificados los activos, es necesario valorar los activos de acuerdo a su relevancia e importancia para la empresa. Para ello se realiza una valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad[31]:

[D]. Disponibilidad, [C]. Confiabilidad, [I].Integridad, [A]. Autenticidad, y [T]. Trazabilidad

Tabla 5. Escala de Valores de Activos

VALORACIÓN CUALITATIVA			CRITERIO
10	Muy alto	[MA]	Daño muy grave para la organización
7 a 9	Alto	[A]	Daño alto para la organización
4 a 6	Medio	[M]	Daño medio para la organización
1 a 3	Bajo	[B]	Daño bajo para la organización
0	Ninguno	[N]	Ningún daño para la organización

Fuente: Magerit V3 libro 2 Catalogo de elementos

[31] Según Magerit V3, Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Teniendo en cuenta la escala de valores (Tabla 6), los criterios y las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad), como la escala estándar (ver anexo D) que sugiere Magerit v3, que permite que se valoren los activos de forma homogénea según el motivo de su importancia, a continuación se indica la valoración para los activos referenciados en la Tabla 5.

Tabla 6. Valoración cualitativa de activos esenciales

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[Vr]. Datos vitales (registros de la empresa)	Bases de datos de usuarios externos.	Confiabilidad	9 [A]	6.pi1, 10.olm, 9.olm, 2.cei.b
		Integridad	10[MA]	6.pi2, 9.olm, 9.lro, 7.cei.c
		Autenticidad	9 [A]	6.pi2, 7.olm, 9.lg.a, 7.lg.a
		Disponibilidad	9 [A]	3.da, 1.pi1, 9.da, 7.da2
		Trazabilidad	6 [M]	1.da, 9.lro, 1.lg
	licencias de funcionamiento	Confiabilidad	9 [A]	6.pi2, 4.pi2, 9.lro, 10.si, 9.cei.b, 5.da
		Integridad	9 [A]	9.olm,
		Autenticidad	6 [M]	9.adm, 6.pi2, 7.lg.a
		Disponibilidad	9 [A]	9.adm, 9.lg.a, 7.da
		Trazabilidad		
	Información de Normativa (Normas locales, nacionales, acuerdos, decretos	Confiabilidad	9 [A]	9.olm, 7.adm
		Integridad	9 [A]	6.pi1, 9.lro
		Autenticidad		
		Disponibilidad	9 [A]	9.da, 5.da2, 3.po
		Trazabilidad		
[Per]. Datos de Carácter personal	Contabilidad de la empresa	Confiabilidad	10[MA]	6.pi1, 5.pi2, 9.lro,
		Integridad	10[MA]	9.olm, 9.adm,
		Autenticidad	9 [A]	1.lg, 6.pi1
		Disponibilidad	10[MA]	9.cei.b, 7.da, 9.adm, 3.cei.c
		Trazabilidad		
[Classified]. Datos clasificados	Ejecutable software Licenciador	Confiabilidad		
		Integridad	6[M]	7.adm, 6.pi2,
		Autenticidad		
		Disponibilidad	9 [A]	3.da, 9.da, 9.olm
		Trazabilidad		

Fuente: esta investigación

Tabla 7. Valoración cualitativa de activos de [D] Datos/ información

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[Files]. Ficheros	**[Files].** Contratos de afiliación de usuarios y del personal que labora en Innovación Global	Confiabilidad	6[M]	5.adm, 3.pi1
		Integridad	3[B]	3.olm, 1.olm, 9.lro
		Autenticidad	3[B]	7.cei.e, 3.lg
		Disponibilidad		
		Trazabilidad		
	[Files]. Matricula de telecomunicaciones para el funcionamiento de Innovación Global	Confiabilidad	3[B]	6.pi1, 5.lg.b
		Integridad		
		Autenticidad	3[B]	7.lg.b, 3.lg, 9.lg.a
		Disponibilidad		
		Trazabilidad		
[backup]. Copias de respaldo	**[backup].** Copias de respaldo y datos de configuración del servidor y de las estaciones de trabajo y puntos de acceso.	Confiabilidad	6[M]	9.olm, 7.adm
		Integridad	6[M]	1.lg, 1.adm, 3.olm
		Autenticidad		
		Disponibilidad	6[M]	5.da, 3.adm
		Trazabilidad		
[Conf]. Datos de configuración	**[Conf].** Datos de configuración del servidor y equipos	Confiabilidad	6[M]	9.olm, 7.adm
		Integridad		
		Autenticidad		
		Disponibilidad	6[M]	5.da, 5.olm,3.adm
		Trazabilidad		
[Password]. Credenciales	**[Password].** Contraseñas de acceso de empleados	Confiabilidad	9[A]	7.olm,3.adm, 2.lg
		Integridad		
		Autenticidad	9[A]	8.lbl,6.pi1, 6.pi2, 9.da
		Disponibilidad		
		Trazabilidad		
[Log]. Registro de actividad	**[Log].** Registros de archivos logs	Confiabilidad	6[M]	3.olm, 5.adm
		Integridad	6[M]	3.adm, 3.olm
		Autenticidad		
		Disponibilidad		
		Trazabilidad		
[acl] datos de control de acceso	**[acl]** datos de control de Acceso	Confiabilidad	9[A]	7.olm,3.adm, 2.lg
		Integridad		
		Autenticidad	9[A]	8.lbl,6.pi1, 6.pi2,9.da
		Disponibilidad		
		Trazabilidad		

Fuente: ésta investigación

Tabla 8. Valoración cualitativa de activos [keys] Claves criptográficas

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[encrypt] claves de cifra**do**	Claves de los APS	Confiabilidad	9[A]	9.adm, 9.lg.b, 6.pi1
		Integridad	9[A]	6.pi1, 9.da.3.cei.b
		Autenticidad	9[A]	8.lbl, 3.cei.d, 6.pi2, 9.si
		Disponibilidad		
		Trazabilidad		

Fuente: esta investigación

Tabla 9. Valoración cualitativa de los [S] Servicios

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[ext]. a usuarios externos (bajo una relación contractual)	**[ext] .** Conectividad a internet y soporte técnico para usuarios externos	Confiabilidad	9[A]	9.lbl
		Integridad	9[A]	9.adm, 9.si, 9.lg.b
		Autenticidad		
		Disponibilidad	9[A]	9.lro, 9.olm
		Trazabilidad		
[int]. interno (a usuarios de la propia organización)	**[int].** Servicio de internet para usuarios internos	Confiabilidad	10[MA]	10.lbl
		Integridad	9[A]	9.si, 9.adm, 9.lg.a
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.da2, 9.olm
		Trazabilidad		

Fuente: esta investigación

Tabla 10. Valoración cualitativa de activo [SW] Software de aplicación

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[os]. Sistema operativo	**[os].** Sisland Server 12.12. Software para controlar y optimizar el servicio de internet en toda la red.	Confiabilidad	8[A]	8.lbl
		Integridad	7[A]	7.adm, 7.lg.a, 7.cei.c
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.da2
		Trazabilidad		

Fuente: esta información

Continuación Tabla 12. Valoración cualitativa de Activo [SW]. Software de aplicación

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
	Windows 8 en equipos de soporte Windows 7 en equipo de soporte	Confiabilidad	9[A]	8.lbl
		Integridad	9[A]	7.adm, 7.lg.a, 7.cei.c
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.da2
		Trazabilidad		
[office].Ofimática	**[office]**.Aplicaciones Ofimáticas. office 2010	Confiabilidad	7[A]	7.lbl
		Integridad		
		Autenticidad		
		Disponibilidad	5[M]	5.da
		Trazabilidad		
[av]. Anti virus	Antivirus Norton en equipos de soporte licenciado	Confiabilidad		
		Integridad	5[M]	5.adm
		Autenticidad		
		Disponibilidad	7[A]	7.olm,7.da
		Trazabilidad		

Fuente: Esta investigación

Tabla 11. Valoración cualitativa de activos de [HW] Equipos informáticos

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[network] soporte de la red	Dispositivos para el funcionamiento de la red inalámbrica:	Confiabilidad	9[A]	9.lbl
		Integridad	5[M]	5.adm, 5.lg.a
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm
		Trazabilidad		
[host] equipo servidor.	Servidor ISP. Computador Intel Dual Core 7 con S.O Sisland Server.	Confiabilidad	9[A]	9.lbl
		Integridad	7[A]	7.adm, 7.lg.a
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm
		Trazabilidad		
[mobile]. informática móvil	Portátil Satellite CL10-B-100.S.O Win8	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm
		Trazabilidad		
[pc] informática personal	Computador Intel Dual Core. S.0 win7	Confiabilidad	7[A]	7.lbl
		Integridad	5[M]	5.adm, 5.pi1
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm
		Trazabilidad		

Fuente: esta información

Continuación Tabla 13. Valoración cualitativa de activos de [HW] Equipos informáticos (hardware)

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[IMP]. Medios de Impresión	**[IMP].** Impresora Epson y Lexmark	Confiabilidad		
		Integridad	3[B]	3.adm
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		

Fuente: Esta investigación

Tabla 12.Valoración Cualitativa de activo [COM] Redes de comunicaciones

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[wifi]. red inalámbrica	Red inalámbrica de Innovación Global	Confiabilidad	10[MA]	10.lbl
		Integridad	9[A]	9.adm, 9.olm
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm, 9.adm
		Trazabilidad		
[LAN]. red local	Red Local	Confiabilidad	10[MA]	10.lbl
		Integridad	9[A]	9.adm, 9.olm
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm, 9.adm
		Trazabilidad		
[Internet]. Internet	Internet	Confiabilidad	10[MA]	10.lbl
		Integridad	9[A]	9.adm, 9.olm
		Autenticidad		
		Disponibilidad	9[A]	9.da, 9.olm, 9.adm
		Trazabilidad		
[mobile]. telefonía móvil	Telefonía móvil	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	1[B]	1.da, 1.adm
		Trazabilidad		

Fuente: esta investigación

Tabla 13.Valoración Cualitativa de activo [Media] Soportes de información

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
Soportes electrónicos [electronic] **[disk]** discos Duros	**[disk].** Unidades de backup de configuraciones de equipamiento inalámbrico, discriminado por carpetas.	Confiabilidad		
		Integridad	5[M]	5.adm, 5.lg.b
		Autenticidad		
		Disponibilidad	3[B]	3.da, 3.olm
		Trazabilidad		
	[disk] . Backup del servidor	Confiabilidad		
		Integridad	7[A]	7.adm, 7.lg.a
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
	[disk]. Backup de la BD usuarios externos	Confiabilidad		
		Integridad	7[A]	7.adm, 7.lg.a
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
Soportes no electrónicos [non_electronic] [**printed**] material impreso	**[printed].** AZ- con los contratos de los usuarios	Confiabilidad	7[A]	7.lbl
		Integridad		
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
	[printed]. AZ- con facturas, soportes contabilidad y licencias	Confiabilidad	7[A]	7.lbl
		Integridad	6[M]	6.pi1
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
	[printed]. Carpetas Varios	Confiabilidad	7[A]	7.lbl
		Integridad	7[A]	7.adm, 7.lg.a
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		

Fuente: esta investigación

Tabla 14. Valoración Cualitativa de activo [AUX] Equipamiento auxiliar

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[ups] sistemas de alimentación ininterrumpida	Ups del servidor, y computadores de soporte	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		
[furniture] mobiliario:	Estantes, armarios, escritorios, archivadores, etc	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		
[power] fuentes de alimentación	Estabilizadores, Fuentes de poder de los equipos de computo	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		
[ac] generadores eléctricos	Planta eléctrica de 1200 W	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		
Cableado**[cabling]**: **.[wire]** cable eléctrico **.[fiber]** fibra óptica	**[wire]** cable de la instalación eléctrica	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
	.[fiber] Cableado estructurado	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		

Fuentes: Esta investigación

Tabla 15. Valoración Cualitativa de activo [L] Instalación

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[building]. Edificio	Infraestructura física, donde se localizan los sistemas de información y comunicación y control de la red de Innovación Global	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	7[A]	7.da, 7.olm
		Trazabilidad		
[mobile].platafo rmas móviles **[car]**	**[car]** vehículo utilizado para transportar al personal de mantenimiento e instalación de la red.	Confiabilidad		
		Integridad		
		Autenticidad		
		Disponibilidad	3[B]	3.da
		Trazabilidad		

Fuente: esta investigación

Tabla 16.Valoración Cualitativa de activo [P] Personal

Código de activo Magerit	Activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio	Importancia según escala estándar
[ui]. usuarios internos	**[ui].** Personal de recepción, área técnica, administrativa y archivo	Confiabilidad		
		Integridad	6[M]	6.pi2
		Autenticidad		
		Disponibilidad	6[M]	6.pi1
		Trazabilidad		
[adm]. administradores de sistemas	Administrador de red.	Confiabilidad		
		Integridad	6[M]	6.pi2
		Autenticidad		
		Disponibilidad	6[M]	6.pi1
		Trazabilidad		
[ue]. usuarios externos	Usuarios que acceden al servicio de internet que provee la empresa	Confiabilidad		
		Integridad	6[M]	6.pi2
		Autenticidad		
		Disponibilidad	6[M]	6.pi1
		Trazabilidad		

Fuente: esta investigación

8.2.3 Caracterización y Valoración de las Amenazas

Las amenazas pueden afectar los activos de una empresa, por ello es importante identificarlas y determinar el nivel de exposición en la que se encuentra cada activo de información en la organización.[32]

En la identificación de las amenazas se tiene en cuenta el catálogo de amenazas posibles para un activo. En el libro II de elementos se indica la clasificación de amenazas en cuatro grupos:[33]

- Desastres naturales(N)
- De origen industrial (I)
- Errores y fallos no intencionados(E)
- Ataques deliberados o intencionados(A).

Cada grupo de amenaza se representa por una letra, así mismo cada grupo presenta unos tipos de amenazas que pueden darse en los activos. A continuación se indican las amenazas que hacen parte de los grupos mencionados.

Tipos de amenazas[34]

[N] Desastres naturales. Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. Pueden ser de origen natural o industrial.

De origen natural o accidental

- [N.1] Fuego
- [N.2] Daños por agua
- [N.*] Desastres naturales

[I] De origen industrial. Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica

---

[32] modulo-SGSI-233003.UNAD
[33] Catálogo de amenazas. Página Magerit V.3 - Libro II - Catálogo de Elementos
[34] Amenazas. Página 25. Magerit_v3_libro2_catálogo de elementos.pdf

- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados. Fallos no intencionales causados por las personas.

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de [re-]encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de información
- [E.20] Vulnerabilidades de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados. Fallos deliberados causados por las personas.

- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10] Alteración de secuencia

- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información
- [A.18] Destrucción de la información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.24] Denegación de servicio
- [A.25] Robo de equipos
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal

8.2.3.1 Valorización de las amenazas

Después de realizar la valoración cualitativa de los activos se procede a evaluar el valor que pierde en caso de que se materialice una amenaza.

De acuerdo al libro 2 Catalogo de elementos de Magerit para realizar la valoración e identificación de las amenazas es necesario determinar la frecuencia con la que ocurren, las dimensiones de seguridad (confiabilidad [C], integridad [I], autenticidad [A], disponibilidad [D] y Trazabilidad [T]) que pueden ser afectadas y una escala de rango porcentual de impactos sobre los activos.

En las tablas 19 y 20 se indican los rangos de frecuencia de amenazas y la escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Tabla 17. Rango de Frecuencia de Amenazas

Valor			Criterio
100	Frecuencia muy alta	FMA	1 vez al día
70	Frecuencia alta	FA	1 vez cada semana
50	Frecuencia media	FM	2 vez cada 2 meses
10	Frecuencia baja	FB	1 vez cada 6 meses
5	Frecuencia media baja	FMB	1 vez al año

Fuente: SGSI. Módulo UNAD

Tabla 18. Escala rango porcentual de impactos

Impacto		Valor
Muy alto	[MA]	100%
Alto	[A]	75%
Medio	[M]	50%
Bajo	[B]	20%
Muy bajo	[MB]	5%

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

8.2.3.2 Valoración de amenazas de los activos de Innovación Global

En la tabla 21 se presenta la frecuencia en que se presentan las amenazas y el valor porcentual de impactos en los activos para cada dimensión de seguridad. La valoración se realiza teniendo la información obtenida mediante charlas informales con personal de la empresa.

Tabla 19. Amenazas, frecuencia e impacto: [D] Datos/ información

Activo de la empresa	Amenazas	Frecuenc	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	T
-Contratos de afiliación e información de usuarios externos a quienes se les provee el servicio de internet. -Datos de contabilidad de la empresa	E1. Errores de los usuarios	10		100%	100%	100%	
	E15. Alteración accidental de la información por usuario interno	5			100%		
	E18. Destrucción de la información	5			100%		
	E19. Fugas de información	5		75%			
	A5. Suplantación de la identidad del usuario	5	100%	100%	100%		
	A6. Abuso de privilegios de acceso	5		75%	75%	75%	
	A11. Acceso no autorizado	5		50%			
	A15. Modificación deliberada de la información	5			100%		
	A19. Revelación de información	10		100%			
Datos de configuración del servidor y de las estaciones de trabajo y puntos de acceso.	E2. Errores del administrador	5		100%	100%	100%	
	E15. Alteración accidental de la información	10			75%		
	E18. Destrucción de la información	5			100%		
	A6. Abuso de privilegios de acceso	10		100%	100%	100%	
	A11. Acceso no autorizado	5		75%			

Activo de la empresa	Amenazas	Frecuenc	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	T
	A15. Modificación deliberada de la información	5			100%		
	A19. Revelación de información	5		75%			
[acl] datos de control de Acceso	E4. Errores de configuración	10			75%		
	A6. Abuso de privilegios de acceso	5		75%	75%	75%	
	A11. Acceso no autorizado	5		100%			

Fuente: ésta investigación

Continuación de la tabla 21. Amenazas, frecuencia e impacto: [D] Datos/ información

Activo	Amenaza	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[Password]. Contraseñas de acceso de empleados	E2. Errores del administrador	5		100%	100%	100%	
	E19. Fugas de información	5		50%			
	A6. Abuso de privilegios de acceso	5		50%	75%	50%	
	A11. Acceso no autorizado	10		75			
	A19. Revelación de información	5		50%			
[Log]. Registros de archivos logs	E2. Errores del administrador	5		100%	100%	100%	
	E3. Errores de monitorización	10			75%		75%
	A13. Repudio	10	20%				
	A19. Revelación de información	5		50%			

Fuente: esta investigación

Tabla 20. Amenazas, frecuencia e impacto: [keys] Claves criptográficas

Activo	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[encrypt] claves de cifra**do** Claves de los APS, estaciones y el servidor. Gestión de llaves	E1. Errores de los usuarios.	5		50%	50%	50%	
	E2. Errores del administrador.	5		50%	50%	50%	
	A6. Abuso de privilegios de acceso	5		50%	75%	50%	
	A11. Acceso no autorizado	5			75%		
	A15. Modificación deliberada de la información	5			100 %		

Fuente: esta investigación

Tabla 21. Amenazas, frecuencia e impacto: [S] Servicios

Activo	Activo de la empresa	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
Internet: a usuarios externos bajo una relación contractual usuarios internos	E1. Errores de los usuarios externos	50		50%	75%	50%	
	E9. Errores de re-encaminamiento	10		50%			
	E10. Errores de secuencia	10			100%		
	E15. Alteración accidental de la información	10			100%		
	E19. Fugas de información	5		50%			
	A5. Suplantación de la identidad del usuario	5	50%	75%	100%		
	A6. Abuso de privilegios de acceso	10		50%	100%	50%	
	A7. Uso no previsto	5		20%	50%	20%	
	A13. Repudio	5			50%		20%
	A15. Modificación deliberada de información	5			100%		
	A18. Destrucción de información	5				100%	
	A19. Revelación de información	5		50%			
	A24. Denegación del servicio	10				100%	

Fuente: esta investigación

Tabla 22. Amenazas, frecuencia e impacto: [SW] Software de aplicación

Activos	Activo de la empresa Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[SO] Sistemas operativos **[av]**. Anti virus	I.5. Avería de origen físico o lógico	50				100%	
	E1. Errores de los usuarios	5		100%	100%	100%	
	E.2 Errores del administrador	5	100%				
	E15. Alteración accidental de la información	10			75%		
	E18. Destrucción de información	5				100%	
	E20.vulnerabilidad de los programas	10		20%	75%	50%	
	E21. Errores de mantenimiento, actualización de programas(software)	10			75%	100%	
	A7. Uso no previsto	10		20%	50%	50%	
	A8. Difusión de software dañino	10		50%	75%	100%	
	A9. Re-encaminamiento de mensajes	5		20%			
	A10. Alteración de secuencia	5			75%		

Fuente: esta investigación

Tabla 23. Amenazas, frecuencia e impacto: [HW] Equipos informáticos

Activo	Activo de la empresa	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[network] soporte de la red Dispositivos para el funcionamiento de la red inalámbrica(antenas, aps, etc) **[pc]** servidor **pc** informática personal	N*. Desastre natural	5				100%	
	I1.fuego origen industrial	5				100%	
	I.3. Contaminación mecánica	50				20%	
	I.4. Contaminación electromagnética	10					
	I.5. Avería de origen físico o lógico	50				75%	
	I.6. Corte del suministro eléctrico	10				100%	
	I.7. Condiciones inadecuadas de temperatura y/o humedad	5				100%	
	I.11. Emanaciones electromagnéticas	10		20%			
	E2. Errores del administrador	5		20%	20%	20%	
	E23. Errores de mantenimiento/ actualización de programas(hardware)	5				20%	
	E24. Caída del sistema por agotamiento de recursos	10				50%	
	E25. Robo	5		50%		75%	
	A6. Abuso de privilegios de acceso	5		50%	100%	50%	
	A7. Uso no previsto	10		20%	50%	50%	

Tabla 24. Amenazas, frecuencia e impacto: [COM] Redes de comunicaciones

Activo	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[wifi]. red inalámbrica **[LAN]**. red local **[Internet]** internet	I.8. Fallo de servicios de comunicaciones	10				100%	
	E2. Errores del administrador	5		100 %	100%	75%	
	E9. Errores de re-encaminamiento	10		75%			
	E15. Alteración accidental de la información	5			50%		
	E18. Destrucción de información	5				75%	
	E24. Caída del sistema por agotamiento de recursos	10				100%	
	A5. Suplantación de la identidad del usuario	5	50%	75%			
	A6. Abuso de privilegios de acceso	5		50%	75%	50%	
	A9. Re-encaminamiento de mensajes	10		50%			
	A10. Alteración de secuencia	5			100%		
	A11. Acceso no autorizado	5			100%		
	A12. Análisis de trafico	5		20%			
	A15. Modificación deliberada de la información	5			75%		
	A19. Revelación de información	5		50%			
	A24. Denegación de servicio	10				100%	

Fuente: esta investigación

Tabla 25. Amenazas, frecuencia e impacto: [Media] Soportes de información

Activos	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[electronic] Soportes electrónicos	N1. Fuego	5				100%	
	N2. Daños por agua.	5				100%	
	I3. Contaminación mecánica	50				100%	
	I4. Contaminación electromagnética	10				75%	
	I5. Avería de origen físico o lógico	50				100%	
	I6. Corte del suministro eléctrico	50				100%	
	I10. Degradación de los soportes de almacenamiento de la información	10				100%	
	I11. Emanaciones electromagnética	10		75%			
	E15. Alteración accidental de la información	10			75 %		
	E18. Destrucción de información	5				100%	

Activos	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
	E23. Errores de mantenimiento/ actualización de equipos(hardware)	5				75%	
	E25. Perdida de equipos			50%		100%	
	A11. Acceso no autorizado	5			75 %		
	A19. Revelación de información	5		50%			
	A22. Manipulación de los equipos	10		50%		75%	
	A25. Robo	5		100%		100%	
	A26. Ataque destructivo	5		50%		50%	
Soportes no electrónicos [non_electronic] [**printed]** material Impreso	N.*2. Daños agua	5		100%		100%	
	I3. Contaminación mecánica	5		50%		50%	
	I7. Condiciones inadecuadas de temperatura y/o humedad	5		20%		20%	
	E1. Errores de los usuarios	5		100%	100 %	75%	

Fuente: esta investigación

Tabla 26. Amenazas, frecuencia e impacto [AUX] Equipamiento auxiliar

Activo	AMENAZAS	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			A	C	I	D	T
[ups] sistemas de alimentación ininterrumpida **[furniture]** mobiliario **[power]** fuentes de alimentación **[ac]** generadores eléctricos Cableado**[cabling]: [wire]** cable eléctrico **[fiber]** fibra óptica	N*. desastre natural	5				100%	
	I1. Fuego origen industrial	5				50%	
	I3. Contaminación mecánica	10				75%	
	I4.Contaminación electromagnética	5				20%	
	I5. Avería de origen físico o lógico	10				50%	
	I6. Corte del suministro de energía	50				75%	
	I7. Condiciones inadecuadas de temperatura y/o humedad	10				50%	
	I9. Interrupción de otros servicios y suministros esenciales	10				50%	
	A22. Manipulación de los equipos	10		20%		20%	
	A26. Ataque destructivo	5				50%	
	A25. Robo	5		75%		100%	

Tabla 27. Amenazas, frecuencia e impacto [L] Instalación

Grupo de Activo	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			A	[C]	[I]	[D]	I
[building]. Edificio **[mobile].p**lata-formas: móviles **[car]**	N*. Desastres naturales	5				100%	
	I*. desastres industriales	5				75%	
	I11. Emanaciones electromagnéticas	10		20%			
	A7. Uso no previsto	10		20%	50%	50%	
	A11. Acceso no autorizado	10			75%		
	A26. Ataque destructivo	5				100%	

Fuente: esta investigación

Tabla 28. Amenazas, frecuencia e impacto: [P] Personal

Grupo de Activo	Amenazas	Frecuencia	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[ui]. Personal de recepción, área técnica, administrativa y archivo **[adm].** Administrador de red.	E19. Fugas de información	5		20%			
	E28. Indisponibilidad del personal	10				75%	
	A29. Extorsión	5		50%	100%	50%	
	A30. Ingeniería social	5		100%	100%	100%	

Fuente: esta investigación

8.2.3.3 Salvaguardas

Las salvaguardas o contra medidas son procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras necesitan seguridad física y, por último, está la política de personal. Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la frecuencia de las amenazas. Llamadas salvaguardas preventivas. Una salvaguarda preventiva ideal mitiga completamente la amenaza.

Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan. Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar.

A continuación se indican las salvaguardas existentes en Innovación Global.

Tabla 29. Protecciones generales u horizontales

Salvaguarda	Dimensión	Valor
[H.I.A]. Identificación y autenticación	[A], [C], [I]	30%
[H.tools] herramientas de seguridad	[I], [D], [C]	20%
[DLP] Herramienta de monitorización de tráfico	[D], [I], [T]	50%

Fuente: esta investigación

[H.I.A] Identificación y autenticación: existen mecanismo de autenticación con medidas básicas para al acceso; con contraseñas que casi no se cambian, donde sus claves son demasiado cortas menos de 8 caracteres y obvios con el nombre de la empresa. Por medio de esta salvaguarda se logra proteger a los activos del tipo hardware es caso los dispositivos inalámbricos y servidor sisland server, sus dimensiones son Autenticidad, Confidencialidad e Integridad para los equipos, con una efectividad del 30%, la valoración se da porque a pesar de existir mecanismos básicos, no son los ideales y pueden ser fácilmente vulnerados.

[H.tools] Herramientas de seguridad: existen herramientas de seguridad con medidas básicas, para detectar puertos abiertos, la existencia de conflictos de ip, detección de ruido en la red. Por medio de esta salvaguarda se protege a los activos de hardware, software, servicios afecta las dimensiones de Integridad, Disponibilidad, Confidencialidad con una efectividad del 20% debido a que no cumplen a cabalidad sus objetivos.

[DLP] Herramienta de monitorización de tráfico: existe un mecanismo que permite la monitorización de los usuarios, identificados por un ID donde se puede observar su comportamiento en la red, el tipo de paquetes que este enviando o recibiendo. Esta salvaguarda protege los activos de hardware, software y servicios; su dimensión es Disponibilidad, Integridad, Trazabilidad con una efectividad de 50% debido a que proporciona mucha información sobre cualquier evento que se presente.

Tabla 30. Protección de los datos/información

Salvaguarda	Dimensión	Valor
[D.A] copia de seguridad de los datos(backup)	[I], [A], [C], [D], [T]	10%

Fuente: esta investigación

[D.A] Copia de seguridad de los datos (backup): actualmente se elaboran copias de seguridad tanto de los equipos inalámbricos como del servidor Sisland server, igualmente se crean copias a los archivos administrativos relacionados con el servicio de internet en un solo equipo, pero se consideran básicos debido a que por cualquier motivo puede ser alterados modificados o borrados; esta salvaguarda se aplica en todas y cada una de las dimensiones; su evaluación es baja ya que no existe un clara política de quien debe administrar estas copias.

Tabla 31. Protección de las aplicaciones (software)

Salvaguarda	Dimensión	Valor
[SW] Copias de seguridad backup	[I], [A], [C], [D], [T]	10%
[WH.CM] cambios(actualizaciones y mantenimiento)	[C], [D], [I]	10%

Fuente: esta investigación

[SW] Copias de seguridad backup: el sistema de la empresa permite generar una copia de seguridad del sistema operativo, igualmente para los dispositivos de equipamiento inalámbrico pero se consideran bajos debido a que no se encuentra completos o los dispositivos son de diferente marca, esta salvaguarda se aplica al software y afecta a las dimensiones [I], [A], [C], [D], [T].

[WH.CM] Cambios (actualizaciones y mantenimiento): actualmente el sistema de equipamiento inalámbrico en sus firmwares ha sido actualizado en las versiones recientes, pero el sistema operativo del servidor sisland server debido su costo no está actualizado; su valor es bajo debido a que no se cuenta con la última versión el servidor y es pieza fundamental en la empresa. Esta salvaguarda

se aplica al software y tiene en cuenta las dimensiones de Confidencialidad, Disponibilidad e Integridad.

Tabla 32. Protección de las comunicaciones

Salvaguarda	Dimensión	Valor
[COM.wifi] Seguridad Wireless	[C], [D],	50%

Fuente: esta investigación

[COM.wifi]. Seguridad Wireless: Se tienen redes inalámbricas que cuentan con cifrado WPA2, WPA, existe control en los protocolos de salida y entrada, se aplica control en ancho de banda y control de uso de aplicaciones p2p, control de acceso por medio de filtro por Mac. Se tiene una relación con las dimensiones de confidencialidad y disponibilidad, su evaluación se debe a que su método de autenticación en la red como el acceso a la misma no son cien por ciento seguros.

8.2.3.4 Estimación del estado del riesgo

En actividad procesan los datos recopilados en las actividades anteriores para analizarlos y evaluar el estado del riesgo

La estimación del estado del riesgo comprende dos tareas: la estimación de impacto y riesgo, el objetivo de ellas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

A continuación se indica la escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo

	MA:	Muy alto
	A:	Alto
	M:	Medio
	B:	Bajo
	MB:	Muy bajo

8.2.3.5 Estimación del impacto

Para determinar el alcance del daño que se produce sobre los activos de información si una amenaza se materializara se debe evaluar el grado de repercusión que se presente en los activos teniendo en cuenta las dimensiones de: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. En la tabla 33 se indica la calificación de los activos

Media: deben ser re-evaluados para mejorar, cambiar o adaptar nuevos controles
Alta y Muy alta: requieren atención urgente.

Tabla 33. Valores estimación de impacto

IMPACTO	Degradación				
	5%	20%	50%	75%	100%
MA	M	A	A	MA	MA
A	B	M	M	A	A
M	MB	B	B	M	M
B	MB	MB	MB	B	B
MB	MB	MB	MB	MB	MB

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos

Impacto acumulado: Impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos y valoración de las amenazas, sin tener en cuenta las salvaguardas actuales. Requieren atención inmediata.

Impacto residual: Resultado de combinar el valor de los activos, la valoración de las amenazas y la efectividad de los salvaguardas aplicadas; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tuvieron en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

En la tabla 34 se indica la valoración de los activos de información de la empresa de Innovación Global teniendo en cuenta las amenazas que podrían causar más daño a los activos de información, este dato se toma de la evaluación de amenazas realizado en el punto 8.2.3.2.

Tabla 34. Valoración de impacto en activos de información

Activo	Amenaza	Impacto Acumulado					Impacto Residual				
		A	C	I	D	T	A	C	I	D	T
[D] Datos/ información	[E.1] Errores de los usuarios										
	[E3]. Errores de monitorización										
	[E.4] Alteración accidental de la información										
[D] Datos/ información	[E15].Modificación deliberada de la información										
	[A6]. Abuso de privilegios de acceso										
	[E18]. Destrucción de la información										
	[A15]. Modificación deliberada de la información										
[S] Servicios	[E9]. Errores de re-encaminamiento										
	[E10]. Errores de secuencia										
	[E15].Alteración accidental de la información										
	[E19]. Fugas de información										
	[A5]. Suplantación de la identidad del usuario										
	[A6]. Abuso de privilegios de acceso										
	[A7]. Uso no previsto										
	[A13]. Repudio										
	[A15].Modificación deliberada de información										
	[A24]. Denegación del servicio										

Fuente: esta investigación

Continuación de la tabla 34 Valoración de impacto en activos de información

Activo	Amenaza	Impacto Acumulado					Impacto Residual				
		A	C	I	D	T	A	C	I	D	T
[SW] Software de aplicación	[E.1] Errores de los usuarios										
	[E.2] Errores del administrador										
	[E.4] Alteración accidental de la información										
	[E.18] Destrucción de información										
	[E21]. Errores de mantenimiento actualización de programas(software)										
	[E20].vulnerabilidad de los programas										
	[I.5]. Avería de origen físico o lógico										
[HW] Equipos informáticos	[N*]. Desastre natural										
	[I1].fuego origen industrial										
	[I.3]. Contaminación mecánica										
	[I.4]. Contaminación electromagnética										
	[I.5]. Avería de origen físico o lógico										
	[I.6]. Corte del suministro eléctrico										
	[I.7]. Condiciones inadecuadas de temperatura y/o humedad										
	[I.11]. Emanaciones electromagnéticas										
	[E2]. Errores del administrador										
	[E23]. Errores de mantenimiento/ actualización de										

Activo	Amenaza	Impacto Acumulado					Impacto Residual				
		A	C	I	D	T	A	C	I	D	T
	programas(hardware)										
	E24. Caída del sistema por agotamiento de recursos										
	[E25]. Robo										
	[A6]. Abuso de privilegios de acceso										
	[A7]. Uso no previsto										
[COM] Redes de comunicaciones	[I.8]. Fallo de servicios de comunicaciones										
	[E2]. Errores del administrador										
	[E9]. Errores de re-encaminamiento										
	[E15]. Alteración accidental de la información										
	[E18]. Destrucción de información										
	[E24]. Caída del sistema por agotamiento de recursos										
	[A24]. Denegación de servicio										
[Media] Soportes de información	[N.*] desastre natural										
	[I3]. Contaminación mecánica										
	[I4]. Contaminación electromagnética										
	[I5.] Avería de origen físico o lógico										
	[I6]. Corte del suministro eléctrico										
	[I10]. Degradación de los soportes de almacenamiento de la información										
	[I11]. Emanaciones electromagnética										
	[E15]. Alteración accidental de la información										

Activo	Amenaza	Impacto Acumulado					Impacto Residual				
		A	C	I	D	T	A	C	I	D	T
[Media] Soportes de información	[E18]. Destrucción de información										
	[E23]. Errores de mantenimiento/ actualización de equipos(hardware)										
	[E25]. Perdida de equipos										
	[A11]. Acceso no autorizado										
	[A19]. Revelación de información										
	[A22]. Manipulación de los equipos										
	[I7]. Condiciones inadecuadas de temperatura y/o humedad										
[AUX] Equipamiento auxiliar	[N*].desastre natural										
	[I1]. Fuego origen industrial										
	[I3]. Contaminación mecánica										
	[I4].Contaminación electromagnética										
	[I5]. Avería de origen físico o lógico										
	[I6]. Corte del suministro de energía										
	[I7]. Condiciones inadecuadas de temperatura y/o humedad										
	[I9]. Interrupción de otros servicios y suministros esenciales										
	[A22]. Manipulación de los equipos										
	[A26]. Ataque destructivo										
	[A25]. Robo										

Fuente: esta investigación

Continuación tabla 34

Activo	Amenaza	Impacto Acumulado					Impacto Residual				
		A	C	I	D	T	A	C	I	D	T
[L] Instalación	[N*.] Desastres naturales										
	[I*]. desastres industriales										
	[I11]. Emanaciones electromagnéticas										
	[A7]. Uso no previsto										
	[A11]. Acceso no autorizado										
	A26. Ataque destructivo										
[P] Personal	[E19]. Fugas de información										
	[E28]. Indisponibilidad del personal										
	[A29]. Extorsión										
	[A30]. Ingeniería social										

Fuente: Esta Investigación

8.2.3.6 Estimación del Riesgo

Para realizar la estimación del riesgo es necesario relacionar el impacto acumulado y frecuencia. La tabla 35 y 36 se indica el rango de frecuencia y el rango porcentual de impactos.

Tabla 35. Rango de frecuencia

Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	mensualmente
1	Normal	FN	1 vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: esta investigación

Tabla 36. Escala rango porcentual de impactos

Impacto		Valor
Muy alto	[MA]	100%
Alto	[A]	75%
Medio	[M]	50%
Bajo	[B]	20%
Muy bajo	[MB]	5%

Fuente: Esta información

En la valoración del riesgo se tienen en cuenta el impacto acumulado, las dimensiones de seguridad y la frecuencia de ocurrencia de las amenazas en relación a los activos. Tabla 37.

Tabla 37. Valoración del riesgo activo [D] Datos/ información

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[E.1] Errores de los usuarios						FN	R1
[E3]. Errores de monitorización						FN	R2
[E.4] Alteración accidental de la información						F	R3
[E15].Modificación deliberada de la información						FN	R4
[A6]. Abuso de privilegios de acceso						PF	R5
[E18]. Destrucción de la información						PF	R6
[A15]. Modificación deliberada de la información						PF	R7

Fuente: esta investigación

Tabla 38. Valoración del riesgo activo [S] Servicios

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
E9]. Errores de re-encaminamiento						FN	R8
[E10]. Errores de secuencia						FN	R9
[E15].Alteración accidental de la información						FN	R10
[E19]. Fugas de información						PF	R11
[A5]. Suplantación de la identidad						PF	R12

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
del usuario							
[A6]. Abuso de privilegios de acceso						FN	R13
[A7]. Uso no previsto						PF	R14
[A13]. Repudio						PF	R15
[A15].Modificación deliberada de información						PF	R16
A24. Denegación del servicio						F	R17

Fuente: esta información

Tabla 39. Valoración del riesgo activo [SW] Software de aplicación

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[E.1] Errores de los usuarios						FN	R18
[E.2] Errores del administrador						PF	R19
[E.4] Alteración accidental de la información						FN	R20
[E.18] Destrucción de información						PF	R21
[E21]. Errores de mantenimiento actualización de programas(software)						F	R22
E20.vulnerabilidad de los programas						FN	R23
[I.5]. Avería de origen físico o lógico						PF	R24

Fuente esta información

Tabla 40. Valoración del riesgo activo [HW] Equipos informáticos

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[N*]. Desastre natural						PF	R25
[I1].fuego origen industrial						PF	R26
[I.3]. Contaminación mecánica						F	R27
[I.4]. Contaminación electromagnética						FN	R28
[I.5]. Avería de origen físico o lógico						F	R29
[I.6]. Corte del suministro eléctrico						F	R30
[I.7] Condiciones inadecuadas de temperatura y/o humedad						PF	R31
[I.11]. Emanaciones						FN	R32

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
electromagnéticas							
[E2]. Errores del administrador						PF	R33
[E23]. Errores de mantenimiento/ actualización de programas(hardware)						FN	R34
[E24.] Caída del sistema por agotamiento de recursos						F	R35
[E25]. Robo						PF	R36
[A6]. Abuso de privilegios de acceso						PF	R37
[A7]. Uso no previsto						FN	R38

Fuente: esta investigación

Tabla 41. Valoración del riesgo activo [COM] Redes de comunicaciones

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[I.8]. Fallo de servicios de comunicaciones						F	R39
[E2]. Errores del administrador						PF	R40
[E9]. Errores de re-encaminamiento						PF	R41
[E15]. Alteración accidental de la información						PF	R42
[E18]. Destrucción de información						PF	R43
[E24]. Caída del sistema por agotamiento de recursos						F	R44
[A24]. Denegación de servicio						F	R45

Fuente: esta investigación

Tabla 42. Valoración del riesgo activo [Media] Soportes de información

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[N.*] desastre natural						PF	R46
[I3]. Contaminación mecánica						F	R47
[I4]. Contaminación electromagnética						PF	R48
[I5]. Avería de origen físico o lógico						F	R49
[I6]. Corte del suministro eléctrico						PF	R50
[I10]. Degradación de los						F	R51

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
soportes de almacenamiento de la información							
[I11]. Emanaciones electromagnética						PF	R52
[E15]. Alteración accidental de la información						PF	R53
[E18]. Destrucción de información						PF	R54
[E23]. Errores de mantenimiento/ actualización de equipos(hardware)						F	R55
[E25]. Perdida de equipos						PF	R56
[A11]. Acceso no autorizado						PF	R57
[A19]. Revelación de información						PF	R58
[A22]. Manipulación de los equipos						PF	R59
[I7]. Condiciones inadecuadas de temperatura y/o humedad						PF	R60

Fuente: esta investigación

Tabla 43. Valoración del riesgo activo [Aux] Equipo auxiliar

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[N*]. desastre natural						PF	R61
[I1]. Fuego origen industrial						PF	R62
[I3]. Contaminación mecánica						FN	R63
[I4].Contaminación electromagnética						PF	R64
[I5]. Avería de origen físico o lógico						FN	R65
[I6]. Corte del suministro de energía						F	R66
[I7]. Condiciones inadecuadas de temperatura y/o humedad						FN	R67
[I9]. Interrupción de otros servicios y suministros esenciales						PF	R68
[A22]. Manipulación de los equipos						FN	R69
[A26]. Ataque destructivo						PF	R70
[A25]. Robo						PF	R71

Fuente: esta investigación

Tabla 44. Valoración del riesgo [L] Instalación

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[N]*. Desastres naturales						PF	R72
[I*]. desastres industriales						PF	R73
[I11]. Emanaciones electromagnéticas						FN	R74
[A7]. Uso no previsto						FN	R75
[A11]. Acceso no autorizado						FN	R76
[A26]. Ataque destructivo						PF	R77

Fuente: Esta Investigación

Tabla 45. Valoración del riesgo activo [P] Personal

Amenaza	Impacto Acumulado					F	Riesgo
	A	C	I	D	T		
[E19]. Fugas de información						PF	R78
[E28]. Indisponibilidad del personal						F	R79
[A29]. Extorsión						PF	R80
[A30]. Ingeniería social						FN	R81

Fuente: Esta Investigación

A continuación se valoran los riesgos teniendo en cuenta su probabilidad de ocurrencia como impacto. Para ello se tiene en cuenta las convenciones de identificación de la tabla 46.

Tabla 46. Probabilidad de ocurrencia e impacto

PROBABILIDAD DE OCURRENCIA	ESCALA IMPACTO
Alta: A	Catastrófico: C
Media: M	Moderado: M
Baja: B	Leve: L

Fuente: Esta investigación

Valoración del riesgo. Para valorar el riesgo se tiene en cuenta la relación entre la probabilidad de ocurrencia y el impacto sobre el activo. En la tabla 47 se indican las convenciones a tenerse en cuenta.

47. Riesgos por impacto y probabilidad

PROBABILIDAD DE OCURRENCIA	ESCALA IMPACTO
Alta: A	Catastrófico: C
Media: M	Moderado: M
Baja: B	Leve: L

Fuente: esta información

Tabla 48. Valoración del riesgo

Activo	Riesgo	Amenaza	Probabilidad			Impacto		
			A	M	B	C	M	L
[D] Datos/ información	R1	[E.1]			X		X	
	R2	[E.3]		X			X	
	R3	[E.4]			X	X		
	R4	[E.15]			X		X	
	R5	[A.6]			X		X	
	R6	[E.18]			X		X	
	R7	[A.15]		X		X		
[S] Servicios	R8	[E.9]			X			X
	R9	[E.10]			X			X
	R10	[E.15]			X	X		
	R11	[E.19]			X			X
	R12	[A.5]			X		X	
	R13	[A.6]		X			X	
	R14	[A.7]			X			X
	R15	[A.13]		X			X	
	R16	[A.15]		X			X	
	R17	[A.24]	X			X		
[sw] software de aplicación	R18	[E.1]			X		X	
	R19	[E.2]			X			X
	R20	[E.4]			X			X
	R21	[E.18]			X		X	
	R22	[E.21]		X			X	
	R23	[E.20]			X		X	
	R24	[I.5]		X			X	
[HW] Equipos informáticos	R25	[N*]			X		X	
	R26	[I.1]			X		X	
	R27	[I.3]		X		X		
	R28	[I.4]			X		X	
	R29	[I.5]		X		X		
	R30	[I.6]	X				X	
	R31	[I.7]		X			X	

Activo	Riesgo	Amenaza	Probabilidad			Impacto		
			A	M	B	C	M	L
	R32	[I.11]			X			X
	R33	[E.2]			X			X
	R34	[E.23]		X			X	
	R35	[E.24]	X			X		
	R36	[E.25]			X		X	
	R37	[A.6]		X			X	
	R38	[A.7]			X			X
[COM] Redes de comunicación	R39	[I.8]	X			X		
	R40	[E.2]			X			X
	R41	[E.9]			X		X	
	R42	[E.15]		X			X	
	R43	[E.18]	X				X	
	R44	[E.24]	X			X		
	R45	[A.24]	X			X		
[Media] Soportes de información	R46	[N*]			X		X	
	R47	[I.3]		X		X		
	R48	[I.4]			X			X
	R49	[I.5]	X				X	
	R50	[I.6]		X			X	
	R51	[I.10]	X				X	
	R52	[I.11]			X			X
	R53	[E.15]			X		X	
	R54	[E.18]			X		X	
	R55	[E.23]	X				X	
	R56	[E.25]			X	X		
	R57	[A.11]			X		X	
	R58	[A.19]			X		X	
	R59	[A.22]			X			X
	R60	[I.7]			X			X
[AUX] Equipo Auxiliar	R61	[N*]			X	X		
	R62	[I.1]			X			X
	R63	[I.3]	X			X		
	R64	[I.4]			X			X
	R65	[I.6]		x			X	
	R66	[I.7]			X			X
	R67	[I.9]		x			x	
	R68	[A.22]			X			X
	R69	[A.26]					X	
	R70	[A.25]			x		X	

Fuente: esta investigación

Continuación tabla 48 Valoración del riesgo

Activo	Riesgo	Amenaza	Probabilidad			Impacto		
			A	M	B	C	M	L
[I] Instalaciones	R71	[N*]			X	X		
	R72	[I*]			X			X
	R73	[I.11]			X			X
	R74	[A.7]			X			X
	R75	[A.11]			X		X	
	R76	[A.26]			X	X		
[P] Personal	R77	[E.19]			X			X
	R78	[E.28]	X			X		
	R79	[A.29]			X		X	
	R80	[A.30]			X	X		

Fuente: esta información

A continuación se relaciona los riesgos de acuerdo a su probabilidad e impacto en los activos

Tabla 49. Matriz de Riesgos

PROBABILIDAD VS IMPACTO	LEVE	MODERADO	CATASTRÓFICO
ALTO		R30,R43,R49,R51,R55,	R17, R35,R39,R44,R45,R63 R78
MEDIO		R2,R13,R15,R16,R22,R24,R29, R31,R34,R37,R42,R47,R50,R65 R67	R7, R27
BAJO	R8,R9,R11,R14,R19,R20, R32,R33,R38,R40,R48, R52,R59,R60,R62,R64,R66 R68,R72,R73,R74	R1,R4,R5,R6,R12,R18,R21,R23, R25,R26, R28,R36, R41,R46,R53,R54,R57, R58,R69,R70,R75,R77,R79	R3,R10,R56,R61,R71, R76, R80

Fuente: esta investigación

8.2.3.7 Análisis de resultados

La empresa Innovación Global, presenta diversas amenazas y vulnerabilidades que pueden colocar en riesgo sus activos de información. De acuerdo a las visitas realizadas, registro fotográfico, resultados de la entrevista, evaluación de sus

activos, pruebas realizada a la red inalámbrica, charlas informales, observación directa y según la valoración de riesgos se identifica lo siguiente:

- Aunque se tiene personal para realizar mantenimiento hardware de tipo preventivo, correctivo y predictivo en los diferentes equipos de la empresa, no se realiza semestralmente y por lo general no se cumple debido a la tardía contratación del personal para este proceso.

- No se tienen definidos procedimientos para realizar mantenimiento correctivo y preventivo a al servidor sisland server y dispositivos inalámbricos como APS y estaciones.

- Ante una falla irrecuperable de hardware en un equipo inalámbrico o del servidor sisland server de uso crítico, no se tienen estipulados planes de contingencia que permitan hacer un proceso de recuperación eficaz de la información.

- El cuarto de telecomunicaciones está lleno de dispositivos que no hacen parte de la red, observándose un desorden y permitiendo una contaminación mecánica que puede afectar a los dispositivos de gran valor como es el servidor sisland server.

- No se definen planes contra la contaminación mecánica especialmente donde se encuentren los dispositivos inalámbricos secundarios como son cargadores tomas entre otros.

- No existe un inventario sobre los dispositivos de red inalámbrica.

- No existe un documento donde se registre la entrada y salida de los dispositivos inalámbricos.

- No existe un plan de actualización de antenas debido a que algunas ya cumplieron con su vida útil.

- No se tiene en cuenta un cambio de frecuencia de algunos aps de 2.4 Ghz a 5 Ghz debido a los problemas de ruido que se han presentado.

- No se contemplan planes y procedimientos cuando se dan de baja equipos inalámbricos, cuando se actualizan o cuando se cambian, sobre todo con la información privada que puedan llegar a contener dichos equipos.

- No cuenta con procedimientos definidos, ni registros de la aplicación de

actualizaciones de software o parches de seguridad en los sistemas de base críticos.

- Es importante que se implementen herramientas de pentesting para verificar vulnerabilidades de la red que pueden materializar un ataque o denegación del servicio.

- No se aplica la norma de cableado estructurado al cuarto de telecomunicaciones en donde no se hace una clasificación de la red de datos y la red eléctrica.

- Es conveniente cambiar el enlace entre las dos torres que tiene la empresa innovación global debido a que se incrementó la capacidad de la red.

- Se debe ampliar el ancho de banda para mejorar el servicio de internet.

- No existen procedimientos para cambiar periódicamente los usuarios y contraseñas de los dispositivos inalámbricos tanto de estaciones como de aps y servidor sisland server.

- En cuanto a las condiciones ambientales y de seguridad en centros de cableado principal y servidores, no se tienen sistemas inteligentes de prevención contra incendios, no existen cámaras de seguridad en dichos sitios, los sistemas de aire acondicionado no siempre se encuentran encendidos, el control de acceso a estos lugares no es tan restrictivo, existe gran cantidad de material como cajas de cartón, muebles de madera y plástico cerca a equipos de comunicación y servidores.

- Existen riesgos en todos los activos de información de la empresa como se constata en la matriz de riesgos.

- Los activos que presentan un alto riesgo son:

  Redes de comunicaciones [COM]
  Datos de información [D]:
  Servicios [S].
  Soportes de información [media]
  Personal [P]
  Equipo auxiliar [Aux]

9. DETERMINACION DE CONTROLES DE SEGURIDAD

9.1 VERIFICACION DE CONTROLES DE SEGURIDAD

Para verificar los controles de seguridad que tiene la empresa de Innovación Global en relación a los que se presentan en la norma ISO 27002: 2013, se procedió a realizar el siguiente checklist (Tabla 30)

Tabla 50 . checklist verificación de controles norma ISO/IEC 27002:2013

Estándar	Aspecto a evaluar	Respuesta		Porcentaje %
		Si	No	
Políticas de seguridad	¿La organización ha definido un documento con la política de seguridad de la información?		x	0%
	¿La política de seguridad de la información se revisa periódicamente?		x	0%
Aspectos organizativos de la seguridad de la información	¿Se han definido las responsabilidades en materia de seguridad de la información?		x	0%
	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?		x	0%
Seguridad ligada a los recursos humanos	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	x		20%
	¿Se comprueban las referencias de todos los candidatos a empleo?	x		50%
Gestión de activos	¿Se dispone de un inventario de activos?	x		10%
	¿Se ha definido quién es el responsable de los activos?	x		10%
Control de accesos	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?		x	0%
	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?		x	0%
	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?		x	0%
	¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión)		x	0%
	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?		x	0%

Continuación de la tabla 50 Checklist

Estándar	Aspecto a evaluar	Respuesta		Porcentaje %
		Si	No	
Seguridad en las telecomunicaciones	¿Existe un proceso de gestión en la red?	x		30%
	¿Hay mecanismos se seguridad pertinentes para gestión de los servicios de red?	x		30%
	¿La organización tiene definidos y cumple Políticas y con los procedimientos de intercambio de información?	x		10%
Adquisición, desarrollo y mantenimiento de los sistemas de información	¿Están documentados los procesos de Análisis y especificación de los requisitos de seguridad?		x	0%
	¿Existen controles que gestionen los recursos y la seguridad de las comunicaciones en servicios accesibles por redes públicas?		x	0%
	¿Existen los mecanismos suficientes apoyados en software y hardware para la Protección de las transacciones por redes telemáticas?		x	0%
Relaciones con suministradores	¿Están establecidos y documentados los procedimientos para Política de seguridad de la información para suministradores?		x	0%
	¿Se registran y monitorean el Tratamiento de riesgos dentro de acuerdos de suministradores?		x	0%
	¿Se conoce y esta documentados los procesos a realizar en una Cadena de suministro en tecnologías de la información y comunicaciones?		x	0%
Gestión de incidentes en la seguridad de la información	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?		x	0%
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?		x	0%
	¿Se han definido, documentado e implantado planes de continuidad de negocio?		x	0%
	¿Los planes de continuidad de negocio se revisan y prueban formalmente?		x	0%
Cumplimiento	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	x		10%
	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	x		10%
	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	x		10%
	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?		x	0%

Fuente: esta investigación

Como puede observarse en tabla 30, los controles de seguridad que se tienen en la empresa de Innovación Global son mínimos respecto a los controles que figuran en la norma ISO 27002:2013. La información obtenida se tiene en cuenta para la elaboración de la declaración de la aplicabilidad donde se indican los controles pertinentes que debería adoptar la empresa para mitigar el riesgo de sus activos de información.

9.2 DECLARACIÓN DE APLICABILIDAD

La declaración de la aplicabilidad se define como 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).[35]

Definido el tratamiento de riesgos, para la empresa y siendo necesario aplicar medidas de seguridad para mitigados los riesgos, se procede al desarrollo de un *SoA*, documento donde se registran los controles de seguridad que son necesarios para la empresa. En la tabla 31 se indican los controles faltantes como aquellos que se deberían tener en cuenta en la empresa de Innovación Global. Anexo C.

[35] http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

10. POLITICAS DE SEGURIDAD

Objetivo: Definir políticas de seguridad para la empresa innovación global de Sibundoy putumayo, que sirvan como estrategias de apoyo para lograr disminuir riesgos, evitar incidentes, mantener la confidencialidad y disponibilidad de sus servicios de forma eficiente y eficaz; que le permitan mantener excelente imagen corporativa.

Políticas de Seguridad para la empresa Innovación Global

Las políticas de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos propios y de los usuarios de la empresa Innovación Global SAS.

Seguridad Interna de la empresa Innovación Global

Toda persona que ingresa a la empresa y es autorizado para el uso de la red inalámbrica y sus diferentes dispositivos haciendo uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas para la seguridad informática.

Del empleado nuevo

Todo el personal nuevo de la empresa, sea contratado por contrato temporal o de manera indefinida, deberá ser notificado al gerente general innovación global, encargado de asignarle los derechos correspondientes (equipo portátil, creación de usuario para la red,) o en caso de retiro de algún empleado, anular y cancelar los derechos otorgados como usuario informático.

Obligación de los empleados

Es responsabilidad cuidar de los bienes empleados de la empresa y servicios informáticos y cumplir las políticas y estándares de seguridad informática.

Capacitación en seguridad informática

Todo nuevo empleado de la empresa innovación global deberá contar con la inducción sobre las políticas y estándares de seguridad informática, donde se den a conocer las obligaciones para los empleados y las sanciones en que pueden incurrir en caso de incumplimiento.

Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la empresa innovación global, o de que se le declare culpable de un delito informático.

Seguridad en el acceso físico de los bienes de Innovación Global

Para el acceso a los sitios y áreas restringidas de la empresa se debe realizar una notificación con el gerente general para la autorización correspondiente, y así proteger la información y los bienes informáticos.

Seguridad en los equipos

El servidor deben ser mantenidos en un ambiente seguro y protegido de:

• Controles de acceso y seguridad física.
• Detección de incendio y sistemas de extinción de conflagraciones.
• Controles de humedad y temperatura.
• Bajo riesgo de inundación.
• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpi da (UPS).

A si mismo los equipos que resguarden información relevante deben ser alimentados por sistemas de potencia eléctrica regulada y estar protegidos por UPS

Protección de la información y de los bienes informáticos de Innovación Global

- El empleado de innovación global deberá reportar de forma inmediata al gerente general cuando se detecte riesgo alguno real o potencial sobre

equipos de red o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- El usuario o funcionario tienen la obligación de proteger los diferentes dispositivos inalámbricos que se encuentren bajo su responsabilidad, aun cuando no se utilicen.

Seguridad en las Áreas de trabajo de Innovación Global

- Las oficinas de los directivos de innovación global así como algunas otras con documentos y activos importantes son áreas restringidas, por lo que solo el personal autorizado por el gerente general puede acceder a él.

- El ingeniero encargado de la empresa será el encargado de generar el resguardo y recabar la firma del empleado de la empresa como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el mismo.

- El portátil y dispositivos inalámbricos asignados, deberá ser para uso exclusivo de las funciones de los empleados o servidores de innovación global para préstamos de sus servicios.

- El empleado de innovación global debe asegurarse que los cables de conexión de los dispositivos inalámbricos no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar una reubicación de cables o del dispositivo como tal al ingeniero encargado.

- Cuando se requiera realizar cambios a los equipos inalámbricos derivado de reubicación de lugares físicos o cambios locativos, éstos deberán ser notificados con gerente general.

- Queda terminantemente prohibido que el empleado o personal distinto al personal de mantenimiento y reparación de equipos inalámbricos destape este dispositivo. Esto acarrea una sanción muy grave.

Mantenimiento de los equipos inalámbricos de Innovación Global

- Únicamente el personal autorizado por el ingeniero encargado de la empresa podrá llevar a cabo los servicios y reparaciones al equipamiento inalámbrico.

- Los empleados deberán asegurarse de respaldar en copias de respaldo o backups de la configuración de los dispositivos inalámbricos como: APs, estaciones de trabajo y servidor.

Perdida de los dispositivos inalámbricos

- El empleado que tenga bajo su responsabilidad o asignados algún dispositivo inalámbrico, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente.

- El usuario que tenga bajo su responsabilidad el dispositivo inalámbrico que hace parte de su instalación para el servicio de internet, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente.

- El empleado y el usuario deberán dar aviso inmediato al ingeniero encargado de la empresa innovación global, y a la oficina que realice el manejo de inventario la perdida, robo o extravío de equipos inalámbricos o accesorios bajo su responsabilidad.

Daño del dispositivo inalámbrico

- El dispositivo inalámbrico que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

De la identificación de incidentes de seguridad en innovación global

- El empleado de la empresa que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al ingeniero encargado de la empresa lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de los encargado de ello, el empleado o persona autorizada para uso del dispositivo inalámbrico deberá notificar al ingeniero encargado.

- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de innovación global debe ser reportado al ingeniero encargado.

Controles para la Generación y Restauración de Copias de Respaldo (Backups) de la configuración de dispositivos inalámbricos innovación global.

- Procedimiento de generación y restauración de copias de respaldo para salvaguardar procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

- Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente de los dispositivos inalámbricos y servidor.

- El empleado de innovación global es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

- Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas. Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.

Planes de contingencia

Son procedimientos internos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen caída del servicio, y estos deben prepararse de cara a futuros sucesos.

- La encargada del soporte técnico debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre.

- Tener en existencia dispositivos inalámbricos de respaldo para la disponibilidad en tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

- Existencia de documentación de los procedimientos detallados para restaurar dispositivos inalámbricos, servidor sisland server, instalación de APS, estaciones entre otros.

Del acceso lógico a los sistemas de Información de Innovación Global

- El empleado es responsable de los mecanismos de control de acceso que les sean proporcionados; Innovación Global maneja login de usuario y contraseña necesarios para acceder a la red en dispositivos inalámbricos como: APs, Sisland Server y toda la información de la infraestructura tecnológica de la empresa, por lo que se deberá mantener de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de innovación global, debe ser proporcionado por el dueño de la información en este caso el gerente general, con base en el principio de “Derechos de Autor” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

- Control de acceso lógico de los empleados a los sistemas de red de la empresa.

- Todos los empleados de la empresa (técnico, ingeniero) son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el ingeniero encargado para poder usar la infraestructura tecnológica y proveer el servicio de internet de innovación global.

- Los empleados no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica innovación global, a menos que se tenga el visto bueno del gerente general de la empresa.

- Cada usuario que acceda a la infraestructura tecnológica de innovación global debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios. Este ID es asignado por el ingeniero encargado.

- Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). No deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

Cláusulas de cumplimiento de las políticas de seguridad para la empresa Innovación Global

El gerente general de innovación global realizará acciones de verificación del cumplimiento del manual de políticas de seguridad informática.

- La oficina encargada podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en estas mismas políticas.

- El gerente general y responsables de los procesos establecidos en innovacion global deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

Violaciones a las políticas de seguridad de innovación global

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el ingeniero encargado de la empresa, realizar pruebas para valorar la seguridad de forma controlada.

- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado

para auto replicarse, dañar o afectar el desempeño o acceso a las redes de innovación global.

SANCIONES

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la Dirección administrativa de la empresa Innovación Global.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al ingeniero encargado hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la empresa.

Todas las acciones en las que se comprometa la seguridad de la Red de y que no estén previstas en esta política, deberán ser revisadas por gerente general para dictar una resolución sujetándose al estado de derecho.

En cuanto a los daños a la infraestructura tecnológica, interceptación ilegítima de sistema informático o red de telecomunicación, Suplantación de sitios web para capturar datos personales, acceso abusivo a un sistema informático y de más delitos informáticos se aplicara la ley 1273, incurriendo a las sanciones que aplica.

Manual de Roles

El ingeniero encargado de Innovación Global tiene como principal responsabilidad la administración y coordinación diaria del proceso de seguridad informática de la empresa.

Tiene como responsabilidad asegurar el buen funcionamiento del proceso de seguridad Informática de la misma.

Debe ser el punto de referencia para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios sobre cómo desarrollar procedimientos para la protección de los recursos.

El ingeniero encargado, es responsable de proponer y coordinar la realización de un análisis de riesgos formal en seguridad de la información que abarque toda la empresa.

Es deber de la oficina el desarrollo de procedimientos de seguridad detallados que fortalezcan la política de seguridad informática.

Es responsabilidad ingeniero encargado, promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

CONCLUSIONES

- La implementación de un SGSI para favorecer no solo la seguridad de la red inalámbrica, sino de todos sus activos de información es una necesidad que la empresa de Innovación Global debe adoptar para garantizar la continuidad de sus servicios. El diseño del SGSI de ser atendido por esta empresa para que pueda garantizar que los riesgos de seguridad que presenta se conozcan, se gestionen y asuman con el fin de que sean minimizados y documentados de forma eficiente para un mejor control de los mismos y así lograr que una continuidad en sus servicios.

- Al identificar los activos de información de la empresa se logra constatar que su manejo no es el más óptimo, esto debido a un exceso de confianza por parte de la administración, al pensar que por tratarse de una empresa pequeña, no esta tan expuesta a riesgos que le perjudiquen como lo que sucede con las grandes empresas. Al respecto se explicó tanto al gerente como al personal de Innovación Global, que sin importar el tamaño de la empresa, esta apreciación es errónea, que las amenazas detectadas pueden materializarse y perjudicar el adecuado funcionamiento de la empresa, que hoy en día es importante que las empresas a diferencia de su tamaño, adopten controles de seguridad para proteger sus activos y sistemas de información.

- Como parte fundamental de la gestión de la seguridad de la información, mediante la metodología de magerit se realizó la identificación de vulnerabilidades y amenazas, para determinar el tratamiento de los riesgos encontrados, los cuales atentan contra la integridad, disponibilidad, confiabilidad, de los servicios que provee la empresa mediante la infraestructura de su red inalámbrica.

- Mediante la declaración de aplicabilidad se determinaron los controles requeridos por la empresa de acuerdo a los riesgos encontrados. Esta declaración de aplicabilidad es un elemento fundamental que se debe tener en cuenta para la implementación de un SGSI, por cuanto relaciona los controles que deben utilizarse en el sistema de gestión.

- Las Políticas de seguridad para la empresa Innovación Global SAS, permiten tener definiciones establecidas que determinan criterios generales para adoptar en distintas funciones y actividades en donde se conocen las

alternativas ante circunstancias repetitivas. Las política de seguridad permite que la empresa adopte normas y procedimientos para regularizar el uso de la información y de los sistemas de información con el fin de mitigar riesgo al que la empresa se vea afectada como por ejemplo accesos no autorizados, deterioros de sus activos, entre otros.

- La norma ISO 27001 y si su anexo A, código de buenas prácticas, son una gran herramienta que permite el establecimiento de políticas, procedimientos y controles que van acordes a los objetivos de la empresa que requiere enfrentar y mitigar el riesgo al pueden enfrentarse sus activos de información.

RECOMENDACIONES

- Debido a las amenazas y vulnerabilidades encontradas en los activos de Innovación Global, es necesario la adopción de un Sistema de Gestión de la Seguridad de la información que le permita tener un mejor control de sus activos de información que le permitan dar continuidad a sus servicios y mantener su clientela.

- Teniendo en cuenta lo observado en la empresa Innovación Global con respecto a su cuarto de telecomunicaciones, en el cual existen diversos elementos que no hacen parte de la red y que además están desordenados. Se sugiere que el espacio utilizado sea exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones.

- Se deben definir planes contra la contaminación mecánica especialmente donde se encuentren los dispositivos inalámbricos secundarios como son: servidor, cargadores tomas entre otros.

- Se debe aplicar la norma de cableado estructurado al cuarto de telecomunicaciones en donde se tenga en cuenta la red de datos y la red eléctrica.

- Debe existir un inventario sobre los dispositivos de red inalámbrica debidamente diferenciados entre los que están funcionando, los nuevos dispositivos y los que están dañados.

- Debe existir un documento donde se registre la entrada y salida de los dispositivos inalámbricos.

- se hace indispensable contar con un manual de configuración de equipos inalámbricos.

- se hace indispensable contar con un manual de instalación de equipos inalámbricos actualizado.

- Se sugiere hacer la respectiva actualización del servidor sisland server a su nueva versión para tener un mejor control de la red.

- Es conveniente cambiar el enlace entre las dos torres que tiene la empresa Innovación Global debido a que se incrementó la capacidad de la red.

- Se sugiere adquirir un sistema de alimentación alterno para el funcionamiento de la red de innovación global.

- Se recomienda ampliar el ancho de banda para mejorar el servicio de internet.

- Se sugiere cambiar periódicamente los usuarios y contraseñas de los dispositivos inalámbricos tanto de estaciones como de aps y servidor sisland server.

- Se recomienda que el personal técnico de innovación global se capacite con un curso de alturas tal como lo exige la ley.

- Es necesario que el personal técnico cuente con elementos de seguridad para el acceso a las antenas.

- Se debe cambiar el tipo de encriptación que utilizan algunos puntos de acceso de WEP a WPA2.

- Es importante que se implementen herramientas de pentesting para verificar vulnerabilidades de la red que pueden materializar un ataque o denegación del servicio.

BIBLIOGRAFÍA

protección de la información y de los datos. (s.f.). Recuperado el 26 de Marzo de 2015, de http://www.mintic.gov.co/portal/604/w3-article-3705.html)

Amenazas a las redes. (s.f.). Recuperado el 7 de septiembre de 2015, de http://www.itesa.edu.mx/netacad/introduccion/course/module1/1.4.3.1/1.4.3.1.html

Areitio Bertolín javier, A. B. (2009). Seguridad en Redes. *Test de penetración y gestión de gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red*, 36-46.

Erb, M. (s.f.). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/about/

Fernández Sánchez Carlos Manuel, P. V. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* Madrid, España: Printed in Spain.

Jaime, C. R. (31 de agosto de 2004). *Redes Inalámbricas.* Obtenido de Redes Inalambricas.Estándares y mecanismos de seguridad: http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

Juan, P. (9 de noviembre de 2014). *incibe*. Obtenido de incibe : https://www.incibe.es/blogs/author/Seguridad/BlogSeguridad/Articulos_seleccionados/?authorID=1002527396

Ley Estatutaria 1266 de 2008. (31 de diciembre de 2008). Recuperado el 24 de Marzo de 2015, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Ley 1341 de 2009. (28 de agosto de 2012). Recuperado el 23 de marzo de 2015, de http://www.enticconfio.gov.co/index.php/enticconfio/item/234-ley-1341-de-2009.htm

Ley 527 de 1999. (s.f.). Recuperado el 24 de Marzo de 2015, de http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/ley_527_1999.pdf

López Neira Agustín, R. S. (2012). *ISO 27000.es*. Obtenido de ISO 27000.es: http://www.iso27000.es/

Manuel, F. C. (2012). La norma ISO 27001 del Sistema de Gestión. *La norma ISO 27001* , 41-44.

Protección Wireless. (s.f.). Recuperado el 7 de septiembre de 2015, de http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

Qué es ISO 27001? (s.f.). Recuperado el 22 de Marzo de 2015, de http://www.iso27001standard.com/es/que-es-iso-27001/

Riesgos Informáticos. (s.f.). Recuperado el 7 de Septiembre de 2015, de http://audisistemas2009.galeon.com/productos2229079.html

Rodrigo, B. (12 de abril de 2012). *isaca.* Obtenido de Implementación efectiva de un SGSI ISO 27001: http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

Seguridad de la red. (s.f.). Recuperado el 7 de septiembre de 2015, de http://www.itesa.edu.mx/netacad/introduccion/course/module1/1.4.3.1/1.4.3.1.html

solarte, F. N. (2014). Riesgos y Control Informático. Obtenido de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

Tecnología inalambrica. (s.f.). Recuperado el 6 de septiembre de 2015, de http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

Tipo de Amenazas. (s.f.). Recuperado el 7 de septiembre de 2015, de https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

ANEXOS

ANEXO A. Autorización de la empresa Innovación Global

innovación global

NIT 900 830133-7

Sibundoy, Putumayo 10 de febrero de 2016

Señores
Universidad Abierta y a Distancia- UNAD
Sede Pasto

Cordial saludo

Mediante la presente "INNOVACIÓN GLOBAL" autoriza a los ingenieros: Doris Esther Jojoa Paz identificada con cédula No. 30.738.884 de Pasto y Karol Martín Córdoba Cuaycal identificado con cedula No. 1.120.216.123 de San Francisco, para continuar con el estudio y análisis de la red de Innovación Global para el proyecto denominado: "Diseño de un sistema de gestión de seguridad de la información SGSI basado en la norma ISO 27001: 2013 para la red inalámbrica de la empresa Innovación Global ubicada en el municipio de Sibundoy Putumayo". Para tal fin se colaborara con la información pertinente y permisos para realizar pruebas de seguridad a la red con la condición de que estas no afecten su integridad, confidencialidad y disponibilidad.

Atentamente,

ROBERTO VALLEJO SANTACRUZ
C.C 5.203.042
Gerente de Innovación Global

ANEXO B. Cuestionario de la entrevista

El siguiente cuestionario está dirigido al personal a cargo del manejo de la red de la empresa de Ingenio Global LTDA.

Objetivo: El presenta cuestionario se realiza con el fin de obtener información para el desarrollo de la propuesta denominada “Diseño de un sistema de gestión de seguridad de la información SGSI basado en la norma ISO 27001:2013 para la red inalámbrica de la empresa Innovación Global ubicada en el municipio de Sibundoy Putumayo”**.** La información recolectada permitirá determinar mejores procesos y controles para la seguridad de la red de la empresa.

CUESTIONARIO

El cuestionario que se presenta a continuación contiene 20 preguntas de tipo cerrado. Responda subjetivamente a cada pregunta.

1. ¿Se cuenta con una estructura organizacional de apoyo para la seguridad de la red y la información?

   Sí__ No___

2. ¿Se ha contado con algún tipo de auditoria que verifique el buen funcionamiento del sistema informático de la empresa?

   Sí___ No___

3. ¿Se cuenta con políticas, normas y procedimientos establecidos para mejorar la seguridad de la red y la protección de la información?

   Sí___ No___

4. ¿Existen planes y programas o procedimientos de seguridad actualizados para garantizar el funcionamiento normal de la red en caso de: incendios, fallas eléctricas, inundaciones, ataques al sistema de información de la empresa, entre otros?

   Sí___ No___

5. Existen planes para prevenir ataques a corto y largo plazo debido a vulnerabilidades posibles en la red física y lógica de la empresa?. En caso de existir, ¿hay un seguimiento de esas vulnerabilidades?

   Sí___ No___

   Observación: _____

6. ¿Se tiene un registro de las transacciones realizadas por los usuarios del sistema?

   Sí___ No___

7. ¿Se cuanta con normas o políticas escrita acerca del uso y responsabilidades de las contraseñas?

   Sí___ No___

8. ¿Existe un registro de los eventos o incidentes que pueden afectar la seguridad de la red y los datos?

   Sí___ No___

9. ¿Se realiza un análisis del tráfico de la red para determinar posibles instrucciones o identificar protocolos que circulen en ella?

   Sí___ No___

10. ¿Se cuenta con un sistema de control de intrusos o IDS?

    Sí___ No___

11. ¿se tiene controles para impedir la propagación de virus y código malicioso, son esporádicos o periódicos?

    Sí___ No___

12. ¿Se efectúan mediciones periódicas del desempeño, capacidad o calidad del servicio de la red?

    Sí___ No___

13. ¿Se conoce en detalle los niveles aceptables de tráfico del servicio de la red para determinar los valores normales del tráfico definido?

    Sí___ No___

14. ¿Existen planes o servicios que describan los procedimientos para recuperar y reanudar el servicio ocasionado por algún incidente en la red que permiten garantizar la continuidad del servicio de la red y sus datos?

    Sí___ No___

15. ¿Se tiene algún tipo de contrato con otra empresa para soporte para solventar problemas respecto a la continuidad de operaciones?

    Sí___ No___

16. ¿La arquitectura de la red está debidamente documentada?

    Sí___ No___

17. ¿Todos los equipos de la red están debidamente identificados y lugar de ubicación es adecuado para los mismos?

    Sí___ No___

18. ¿Se tiene por escrito las normas que regulan la disposición del cableado de red y de la energía eléctrica?

    Sí___ No___

19. ¿Se tienen políticas escritas y claras que orienten el acceso físico a la infraestructura de la red, servicios de internet por parte de los usuarios del sistema?

    Sí___ No___

20. ¿Se ofrecen capacitaciones al personal a cargo de la red que favorezca la seguridad y buen funcionamiento de la red y lo que esta concierne?

    Sí___ No___

ANEXO C. Declaración de Aplicabilidad

En la presente declaración se presenta los controles relevantes para el SGSI de la empresa Innovación Global. Esta declaración se justifica la exclusión de algunos de los controles.

Estado	Abreviatura
Parcialmente	(P)
Parcialmente implementado	(PI)
Totalmente implementado	(TI)
No aplica	(NA)

SECCIÓN	Controles según la norma ISO/IEC 27002	Aplicabilidad (Sí/No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
5	Política de seguridad					
5.1	Directrices de la dirección en seguridad de la información.					
5.1.1	Políticas para la seguridad de la información.	Si	Las políticas de seguridad de la información garantizan compromiso ineludible de protección a la misma frente a una amplia gama de amenazas.	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	La empresa establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del SGSI.	P
5.1.2	Revisión de las políticas para la seguridad de la información	Si	Es conveniente revisar seguidamente las políticas de seguridad para verificar el cumplimiento de las mismas.	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	Mantener una revisión de las políticas de seguridad de la información.	P
6	Organización de la seguridad de la información					
6.1	Organización interna					

6.1.1	Asignación de responsabilidades para la SI.	Si	Los empleados de innovación global que tiene acceso a la información pero deben contribuir de manera exhaustiva al mejoramiento de la seguridad dentro de la empresa.	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	Se realizaran planes de capacitación para el personal a cargo del manejo de la información.	PI
6.1.2	Segregación de tareas	Si	Se tendrá en cuenta el personal autorizado para tenga acceso a la información.	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Políticas de manejo de privilegios sobre la información.	PI
6.1.3	Contacto con las autoridades	Si	La información debe ser manipulada de acuerdo a las políticas de seguridad por medio de canales de comunicación seguros para evitar incidencias.	Se deberían mantener los contactos apropiados con las autoridades pertinentes	Disponer de canales seguros para la administración de la información.	PI
6.1.4	Contacto con grupos de interés especial	Si	El cumplimiento de los objetivos y alcances del SGSI se debe precisar políticas internas para la protección de la información que deben ser conocidas por todos los empleados de innovación global.	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Políticas para la administración de la información al interior de la empresa.	PI
6.1.5	Seguridad de la información en la gestión de proyectos					N/A
6.2	Dispositivos móviles y teletrabajo					

6.2.1	Política para dispositivos móviles	Si	Se hace necesaria la definición de políticas de protección en cuanto a recursos móviles.	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Definir políticas para el manejo de dispositivos móviles.	P
6.2.2	Teletrabajo					N/A
7	Seguridad de los recursos humanos					
7.1	Antes de asumir el empleo					
7.1.1	Selección	Si	Para contratar al personal se deben evaluar las cualidades profesionales, nivel de ética y compromiso con la empresa innovación global.	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Se cuenta con políticas de contratación.	TI
7.1.2	Términos y condiciones del empleo	Si	Es preciso que los nuevos empleados conozcan políticas y responsabilidades en cuanto a sus funciones y manejo de la información	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Se cuenta con políticas de contratación.	TI
7.2	Durante la ejecución del empleo					
7.2.1	Responsabilidades de la dirección	Si	Se debe asegurar que las políticas diseñadas para el manejo de la información sean	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la	Definir políticas de manejo de la información, seguidas de planes de	PI

			cumplidas por los empleados de innovación global	información de acuerdo con las políticas y procedimientos establecidos por la organización	capacitación. .	
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Si	Se debe tener en cuenta las políticas de seguridad de la información al interior de innovación global.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Procedimientos de capacitación en políticas de seguridad de la información.	PI
7.2.3	Proceso disciplinario	Si	Se debe tener en cuenta por las posibles sanciones por incumplimiento de las políticas de seguridad, el mal manejo de la información que pongan en riesgo la y deben ser conocidas por todos los empleados de la empresa.	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Procedimientos de capacitación en políticas de seguridad de la información.	P
7.3	Terminación o cambio de empleo					
7.3.1	Terminación o cambio de responsabilidades de empleo	Si	Es preciso garantizar que después de la finalización de un contrato interno, la información que maneja esta persona no se vea afectada o divulgada.	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar	implementación de políticas de manejo de privilegios sobre la información.	P

				al empleado o contratista y se deberían hacer cumplir.		
8	Gestión de activos					
8.1	Responsabilidad por los activos					
8.1.1	Inventario de activos	Si	Identificar los activos de acuerdo a su grado de importancia dentro de innovación global, en la que se debe tener claro que los activos más relevantes son: el servidor, aps y estaciones.	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	Se debe hacer una clasificación de los activos y establecer el nivel de importancia de los mismos.	P
8.1.2	Propiedad de los activos	Si	Los activos dentro de la empresa deben tener relacionado un responsable de la seguridad.	Los activos mantenidos en el inventario deberían tener un propietario.	Se asignan responsables tanto para los activos de información por medio del área de sistemas y también, para activos físicos que forman parte de los sistemas de información.	TI
8.1.3	Uso aceptable de los activos	Si	Políticas sobre manejo de la información deben admitir tener claridad acerca del uso y manejo adecuado de activos.	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Políticas manejo de activos.	PI

8.1.4	Devolución de activos	Si	Se tiene en cuenta protocolos que garanticen que un empleado haga entrega de los activos que tiene a su cargo y se incluya en el inventario de activos.	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Mecanismos para la devolución de activos.	PI
8.2	Clasificación de la información					
8.2.1	Clasificación de la información	Si	La información debe ser clasificada de acuerdo a su importancia para establecer los controles adaptados al manejo de la misma.	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Mecanismos de prioridades en el manejo de la información.	PI
8.2.2	Etiquetado de la información	Si	Cada información debe ser identificada para que cada persona conozca su naturaleza respete su nivel de confidencialidad, es decir debe ser etiquetada relacionando sus restricciones.	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Políticas de acceso a la información.	PI
8.2.3	Manejo de activos	Si	Los activos deben ser manejados de acuerdo al uso de la información y adaptado a la organización	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Definir políticas para el manejo de activos especificando su utilidad	PI

8.3	Manejo de los soportes de almacenamiento.					
8.3.1	Gestión de medios removibles	Si	No se debe permitir el uso de medios informáticos removibles para evitar fugas y amenazas que puedan tener.	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Definir políticas para que la información no sea extraída	PI
8.3.2	Disposición de los medios	Si	Se debe tener cuenta debido a que son medios que pueden revelar información importante de la empresa	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.	Definir mecanismos para la disposición de los medios	P
8.3.3	Transferencia de medios físicos	Si	Se debe tener cuenta debido a que son medios que pueden revelar información importante de la empresa	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	Definir mecanismo de seguridad cuando un medio físico este en transito	P
9	Control de acceso					
9.1	Requisitos del negocio para control de acceso					
9.1.1	Política de control de acceso	Si	Basado en los servicios que presta innovación global que es el servicio de internet, se deben establecer políticas de control de acceso.	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Tener en cuenta políticas para el control de acceso teniendo en cuenta las áreas críticas.	PI
9.1.2	Política sobre el uso de los servicios de red	Si	Se debe tener en cuenta porque el fuerte de la empresa porque permite	Solo se debería permitir acceso de los usuarios a la	Política de seguridad sobre los servicios de red	PI

			brindar sus servicios a los usuarios.	red y a los servicios de red para los que hayan sido autorizados específicamente.		
9.2	Gestión de acceso de usuarios					
9.2.1	Registro y cancelación del registro de usuarios	Si	Es importante gestionar los usuarios porque son asignados al servidor y permitirá llevar un mejor control en el sistema sin generar problemas de seguridad.	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Definir políticas para el ingreso o eliminación de usuarios del sistema.	PI
9.2.2	Suministro de acceso de usuarios	Si	Es importante gestionar los usuarios porque son asignados al servidor y permitirá llevar un mejor control en el sistema sin generar problemas de seguridad teniendo en cuenta sus privilegios.	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Definir políticas para el acceso a usuarios al sistema	PI
9.2.3	Gestión de derechos de acceso privilegiado	Si	Innovación global garantizar que cada usuario tenga acceso al sistema de información basado en privilegios.	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Definir políticas para la gestión de privilegios.	PI
9.2.4	Gestión de información de autenticación secreta de usuarios					N/A
9.2.5	Revisión de los derechos de acceso de usuarios	Si	Se debe confirmar que los usuarios puedan acceder sólo a los sistemas que tienen permiso.	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	Políticas para la verificación regular del acceso a sistemas de información.	PI

9.2.6	Retiro o ajuste de los derechos de acceso	Si	Se debe confirmar que los usuarios se les administre el retiro o ajuste de los derechos de acceso	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	Políticas para la administración de acceso a sistemas de información.	PI
9.3	Responsabilidades de los usuarios					
9.3.1	Uso de la información de autenticación secreta					N/A
9.4	Control de acceso a sistemas y aplicaciones					
9.4.1	Restricción de acceso Información	Si	Restringir el acceso a los sistemas en especial a servidor el cual administra la red y gestiona el ancho de banda para ofrecer el servicio de internet.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	Establecer controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan diferentes entornos.	PI
9.4.2	Procedimiento de ingreso seguro	Si	Se debe tener un mecanismo de ingreso seguro debido a que el servidor y los dispositivos inalámbricos son accedidos por medio de sesiones atreves de su firmware y sistema operativo.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	Definir política de seguridad al inicio de cada sesión en firmwares e servidor.	P
9.4.3	Sistema de gestión de contraseñas	Si	Es importante gestionar las contraseñas porque por medio de ella se accede al servidor y demás dispositivos inalámbricos.	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	Definir políticas de seguridad a la gestión de contraseñas.	P
9.4.4	Uso de programas utilitarios privilegiados	Si	Se debe tener en cuenta mecanismos que controlen el uso de programas utilitarios porque pueden afectar la	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el	Definir políticas de seguridad al uso de programas utilitarios privilegiados.	P

			seguridad de la información y dispositivos.	sistema y los controles de las aplicaciones.		
9.4.5	Control de acceso a códigos fuente de programas					N/A
10	Criptografía					
10.1	Controles criptográficos					
10.1.1	Política sobre el uso de controles criptográficos	Si	Es necesario contar con políticas de protección de la información en la conexión del usuario.	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Establecer políticas de protección de la información.	PI
10.1.2	Gestión de llaves					N/A
11	Seguridad física y del entorno					
11.1	Áreas seguras					
11.1.1	Perímetro de seguridad física	Si	Es importante garantizar la seguridad de las zonas que manejan información sensible (archivo físico, ubicación de servidor, equipos, almacenamiento copias de seguridad entre otros).	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	Políticas de control de acceso físico a áreas que contienen información sensible.	PI
11.1.2	Controles físicos de entrada	Si	Se debe tener en cuenta al personal autorizado debe acceder a áreas que contengan activos sensibles	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Políticas de control de acceso físico a áreas que contienen información sensible.	PI
11.1.3	Seguridad de oficinas, recintos e instalaciones	Si	En oficinas al interior de innovación global se puede tener acceso a información sensible por lo cual se debe aplicar	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Políticas control de acceso físico.	PI

			controles de seguridad			
11.1.4	Protección contra amenazas externas y ambientales	Si	Garantizar que ninguna amenaza ambiental externa pueda generar daño sobre la información.	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Protección contra factores ambientales como temperatura, humedad, entre otros.	PI
11.1.5	Trabajo en áreas seguras	Si	Las áreas en donde se desarrollan las actividades deben cumplir con estándares de seguridad los cuales inciden tanto para equipos como para el personal.	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	Comprobación del nivel de seguridad de las áreas de trabajo.	PI
11.1.6	Áreas de despacho y carga					N/A
11.2	Equipos					
11.2.1	Ubicación y protección de los equipos	Si	Se debe tener en cuenta protecciones contra daños ambientales, especialmente para el servidor que se maneja al interior de la empresa.	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	Definir controles para el control de factores ambientales como humedad, polvo, entre otros.	PI
11.2.2	Servicios de suministro	Si	La seguridad de los equipos depende de los controles para la protección antes fallas eléctricas, porque un fallo de energía puede dejar inutilizable un equipo o no permite la conexión de los usuarios u otros.	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Implementar nuevas Ups porque las que se cuenta no funcionan bien	PI
11.2.3	Seguridad del cableado	Si	Se debe garantizar que	El cableado de potencia y	Implementar y auditar	PI

			las redes de datos y la inalámbrica no se vean afectada su integridad y confidencialidad de los datos que transportan.	de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	los sistemas de cableado existentes.	
11.2.4	Mantenimiento de equipos	Si	La empresa debe realizar mantenimiento periódico de los equipos como política interna de la misma.	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas	Definir planes de mantenimiento de equipos al interior de la empresa.	PI
11.2.5	Retiro de activos	Si	Se debe garantizar el retiro de activos siempre cuando sea autorizado y registrarse en el inventario de la empresa	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	Definir procedimientos para retiro de activos	PI
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Si	Se garantiza que los activos y equipos que están fuera cuenten con una previa seguridad ante un posible riesgo.	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Definir políticas de seguridad para activos fuera de las instalaciones	PI
11.2.7	Disposición segura o reutilización de equipos	Si	Cuando se cuente con un equipo con información almacenada y este no es utilizado o este de baja puede comprometer la confidencialidad de la empresa.	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	Definir políticas para el proceso de baja de equipos.	PI

11.2.8	Equipos de usuario desatendidos					N/A
11.2.9	Política de escritorio limpio y pantalla limpia					N/A
12	Seguridad de las operaciones					
12.1	Procedimientos operacionales y responsabilidades					
12.1.1	Procedimientos de operación documentados	Si	Garantizar la continuidad de procesos se debe contar con bitácoras que permitan conocer los procedimientos operacionales especialmente los que tengan que ver con activos esenciales.	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Definir políticas para la documentación de procedimientos.	PI
12.1.2	Gestión de cambios	Si	Es importante tener claridad de quienes serán los encargados de realizar el proceso de administración de la información.	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Definir políticas de manejo de privilegios sobre la información.	PI
12.1.3	Gestión de capacidad	Si	Es importante proyectar la empresa a un futuro cambio si se incrementa el número de usuarios aumentando en rendimiento e infraestructura tecnológica.	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Definir un mecanismo donde se tenga en cuenta la gestión de la capacidad	PI

12.1.4	Separación de los ambientes de desarrollo, pruebas y operación					N/A
12.2	Protección contra códigos maliciosos					
12.2.1	Controles contra códigos maliciosos	Si	Es importante tener controles que garanticen que códigos maliciosos no terminen afectando el sistema.	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Definir mecanismos de seguridad para garantizar el control lógico al interior de la empresa.	PI
12.3	Copias de respaldo					
12.3.1	Respaldo de información	Si	Proteger la información garantiza que ante cualquier problema de seguridad se tendrá una fácil recuperación de la información.	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Backups regulares de la información y equipos inalámbricos e servidor sisland server.	PI
12.4	Registro y seguimiento					
12.4.1	Registro de eventos	Si	Es importante tener un registro de eventos porque se podría implementar acciones ante cualquier situación.	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Definir mecanismos para el registro de eventos.	PI
12.4.2	Protección de la información de registro	Si	Es importante tener un control sobre los registros de actividad para que no puedan ser alterados.	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	Definir políticas de implementación y control de registros de actividad.	P

12.4.3	Registros del administrador y del operador	Si	Se debe tener en cuenta la actividad de quienes tengan mayores privilegios sean monitoreados.	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	Definir políticas de implementación y control de registros de actividad.	P
12.4.4	sincronización de relojes	Si	Todos los sistemas estén sincronizados para que cualquier registro coincida en tiempos y se pueda hacer la trazabilidad del mismo.	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	Definir políticas de implementación y control de registros de actividad.	
12.5	Control de software operacional					
12.5.1	Instalación de software en sistemas operativos					N/A
12.6	Gestión de la vulnerabilidad técnica					
12.6.1	Gestión de las vulnerabilidades técnicas	Si	Se debe verificar constantemente las vulnerabilidades que puedan presentar los sistemas o tecnologías usadas dentro de la empresa.	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Definir políticas para la gestión de vulnerabilidades de aplicaciones o sistemas usados por la empresa.	P
12.6.2	Restricciones sobre la instalación de software					N/A

12.7	Consideraciones sobre auditorias de sistemas de información					
12.7.1	Información controles de auditoría de sistemas	Si	Es importante tener control sobre los procedimientos de auditoría desarrollados al interior de la empresa sobre sistemas en funcionamiento.	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Definir políticas para el desarrollo de procesos de auditoria.	P
13	Seguridad de las comunicaciones					
13.1	Gestión de la seguridad de las redes					
13.1.1	Controles de redes	Si	Es necesario que la red inalámbrica que maneja la empresa sea controlada.	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	Definir políticas de administración y uso de redes.	PI
13.1.2	Seguridad de los servicios de red	Si	Es importante tener políticas que permitan la definición de acuerdos sobre el manejo de las redes y servicios que posea.	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	Definir políticas de administración y uso de redes.	PI
13.1.3	Separación en las redes	Si	Es importante separar servicios, usuarios, sistemas en grupos para la red para tener un mejor manejo de la misma y podrá facilitar la	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	Definir mecanismos donde se presente la separación en las redes	PI

			operabilidad si se presenta alguna falla			
13.2	Transferencia de información					
13.2.1	Políticas y procedimientos de transferencia de información	Si	Se debe garantizar que la información se encuentre segura al ser transferida haciendo uso de diferentes mecanismos de protección.	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	Diseñar políticas e implementar controles para la transferencia de información	PI
13.2.2	Acuerdos sobre transferencia de información	Si	Se debe tener claridad de la forma como se puede compartir información al interior de la empresa.	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	Definir políticas e implementar controles para el intercambio seguro de información.	P
13.2.3	Mensajería electrónica					N/A
13.2.4	Acuerdos de confidencialidad o de no divulgación					N/A
14	Adquisición, desarrollo y mantenimientos de sistemas					
14.1	Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Si	Se debe tener en cuenta que todo nuevo sistema de seguridad especifique los controles necesarios para su implementación.	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Definir políticas para la integración de sistemas de información.	P
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Si	Es importante porque se protege la información ante una posible modificación externa en este caso redes públicas.	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de	Definir políticas para los servicios de aplicaciones en redes publicas	P

				actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		
14.1.3	Protección de transacciones de los servicios de las aplicaciones					N/A
14.2	Seguridad en los procesos de desarrollo y soporte					
14.2.1	Política de desarrollo seguro					N/A
14.2.2	Procedimientos de control de cambios en sistemas	Si	Es importante tener procedimientos para el control de cambios en sistemas por permite llevar un inventario de los activos y su funcionalidad en la empresa.	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	Definir mecanismos de control de cambio en sistemas	P
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación					N/A
14.2.4	Restricciones en los cambios a los paquetes de software					N/A
14.2.5	Principios de construcción de sistemas seguros					N/A
14.2.6	Ambiente de desarrollo seguro					N/A
14.2.7	Desarrollo contratado externamente					N/A
14.2.8	Pruebas de seguridad de sistemas					N/A
14.2.9	Prueba de aceptación de sistemas					N/A
14.3	Datos de prueba					
14.3.1	Protección de datos de prueba					N/A
15	Relación con los proveedores					
15.1	Seguridad de la información en las relaciones con los proveedores					
15.1.1	Política de seguridad de la información para las relaciones con proveedores					N/A
15.1.2	Tratamiento de la seguridad dentro					N/A

	de los acuerdos con proveedores					
15.1.3	Cadena de suministro de tecnología de información y comunicación					N/A
15.2	Gestión de la prestación de servicios con los proveedores					
15.2.1	Seguimiento y revisión de los servicios de los proveedores					N/A
15.2.2	Gestión de cambios en los servicios de proveedores					N/A
16	Gestión de incidentes de seguridad de la información					
16.1	Gestión de incidentes y mejoras en la seguridad de la información					
16.1.1	Responsabilidad y procedimientos	Si	Es importante tener procedimiento ante cualquier falla en los sistemas y la persona que esté a cargo	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Definir mecanismo contra fallas y personas que estén a cargo	PI
16.1.2	Reporte de eventos de seguridad de la información	Si	Se deben disponer canales de comunicación que permitan dar a conocer eventos de seguridad que afecten la empresa.	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
16.1.3	Reporte de debilidades de seguridad de la información	Si	Es importante conocer las debilidades de la información para tener presente mecanismo que mitigen esas posibles fallas	Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI

16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos					N/A
16.1.5	Respuesta a incidentes de seguridad de la información					N/A
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Si	Se debe poder establecer el costo de un evento de seguridad de la información.	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
16.1.7	Recolección de evidencia	Si	Es importante tener mecanismos para determinar la forma como se debe actuar contra personas que se les compruebe la generación de eventos de seguridad informática.	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio					
17.1	Continuidad de seguridad de la información					
17.1.1	Planificación de la continuidad de la seguridad de la información	Si	Es importante contar con procesos de seguridad de la información que aseguren la continuidad del negocio al interior de la empresa.	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Establecer políticas de seguridad de la información que garanticen la continuidad del negocio.	P
17.1.2	Implementación de la continuidad de la seguridad de la información	Si	Contar con planes de contingencia que permitan la recuperación del negocio ante cualquier	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y	Establecer políticas de seguridad de la información que garanticen la	P

			evento que ponga en riesgo la información.	controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	continuidad del negocio.	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	Se deben verificar y revisar los planes de continuidad garantizando seguridad con los requerimientos del negocio.	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecida e implementada, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Establecer políticas de seguridad de la información que garanticen la continuidad del negocio.	P
17.2	Redundancias					
17.2.1	Disponibilidad de instalaciones de procesamiento de información.					N/A
18	Cumplimiento					
18.1	Cumplimiento de requisitos legales y contractuales					
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Si	Se tiene en cuenta que la empresa sea consciente de sus obligaciones legales para garantizar el cumplimiento de las mismas.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Establecer políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.	P
18.1.2	Derechos de propiedad intelectual					N/A
18.1.3	Protección de registros	Si	Es importante garantizar la integridad de los registros importantes para evitar cualquier pérdida	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y	Establecer políticas que permitan el cumplimiento de los requerimientos de	PI

			de información.	liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio	carácter legal por parte de la empresa.	
18.1.4	Privacidad y protección de datos personales	Si	Es importante garantizar la protección de los datos en concordancia con requerimientos de carácter legal y que mucha de la información que maneja tiene esta característica.	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	Establecer políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.	PI
18.1.5	Reglamentación de controles criptográficos					N/A
18.2	Revisiones de seguridad de la información					
18.2.1	Revisión independiente de la seguridad de la información	Si				N/A
18.2.2	Cumplimiento con las políticas y normas de seguridad		El gerente general debe asegurarse de que los procedimientos de seguridad se realicen adecuadamente.	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Inspeccionar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.	P
18.2.3	Revisión del cumplimiento técnico	Si	Se debe tener en cuenta que los procedimientos de seguridad estén en concordancia con los estándares definidos para los mismos.	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	Inspeccionar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.	P