FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS.

EVALUACIÓN DE VULNERABILIDADES DE SEGURIDAD EN LA EMPRESA BOOKNOWLEDGE. SOLUCIONES PARA MITIGAR LAS VULNERABILIDADES ENCONTRADAS BAJO LA NORMA ISO 27001:2013. CASO: EMPRESA BOOKNOWLEDGE.

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de TECNOLOGIA EN REDES Y TELECOMUNICACIONES

Profesor guía
Ing. Patricio Arellano.

Autora
Andrea Verónica Murillo Chiriboga.

Año
2017

DECLARACIÓN DE PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientado a sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Patricio Arellano Vargas.

CI: 1706996442

DECLARACIÓN DE PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Fabian Wladimiro Basantes Moreno.

CI: 1709767667

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

Andrea Verónica Murillo Chiriboga.

CI: 1715659270

“AGRADECIMIENTOS”

Quiero expresar mi entero agradecimiento en primer lugar a Dios por haberme dado el don de la perseverancia para alcanzar esta meta. Y a la empresa Booknowledge por permitirme desarrollar este proyecto de titulación en especial a la Arq. Lorena Ganchala y al Ing. Jorge Luis Macas por su colaboración y su predisposición para el término de este trabajo.

De igual manera quiero agradecer al Ingeniero Patricio Arellano por ser mí tutor y solventar todo tipo de dudas siendo un aporte muy importante en la elaboración de este proyecto de titulación, así como también a la Universidad de las Américas y a todos mis profesores.

Finalmente, a todos mis compañeros de estudio, con quienes hemos compartido muchas enseñanzas y logros en todos estos años, y no solo recorrimos este camino juntos, sino que me ayudaron a construir mi presente.

“DEDICATORIA”

A Dios, a mi mami Mirian a mi mamita Fanny a mi papito Guillermo a mi tía Paula quienes siempre han confiado en mí y me han dado su apoyo incondicional, a mi familia y a todas las personas que me ayudaron para culminar mi carrera.

A mi tutor de Tesis el Ing. Patricio Arellano por su gran ayuda y colaboración.

RESUMEN

El actual proyecto de titulación se enmarca en el diseño de un sistema de gestión de la seguridad de la información establecido en la norma ISO/IEC 27001:2013 para el centro de datos de la empresa Booknowledge.

El punto de inicio fue conocer la actualización de la norma ISO/IEC 27001:2013 para tener en cuenta los nuevos objetivos de control y controles a ser implementados, consecutivamente de ello se perpetuó con el reconocimiento del centro de datos de la compañía para definir los activos de la información, y tener claro las amenazas o ataques de los que logran ser víctimas estos activos, así como también se realizó un análisis de los riesgos para precisar el criterio de mitigación de los mismos.

El progreso del SGSI se lo hizo mediante la arquitectura de procesos denominada PDCA, tomando en cuenta que el análisis realizado es utilizando la estimación Cualitativa del Riesgo - Método Triple Criterio – PGV, el cual conlleva a precisar un espectro de amenazas que han sido divididas en tres grandes grupos que son las amenazas humanas, tecnológicas y naturales.

Finalmente, el actual proyecto de titulación sujeta varias tablas que detallan información importante a ser tomada en cuenta en donde las más notables serán aquellas en las cuales se evidencia la aplicación de los controles a las amenazas detectadas, y dos simulaciones de una nueva red LAN de la compañía y de una red corporativa que unificará a la oficina matriz con sus sucursales, ambas serán redes convergentes de voz y datos.

ABSTRACT

This graduation project is part of the design of an information security management system based on ISO / IEC 27001: 2013 for Booknowledge.

The starting point was to know the update of the ISO / IEC 27001: 2013 to reflect the new control objectives and controls to be implemented, then it continued with the reconnaissance of company to define the information assets, and have found threats or attacks that can be victims as well as a risk analysis was also performed to define the criteria for mitigating them.

The system development was did through the process architecture called PDCA, considering that the analysis is conducted using estimation qualitative risk – Triple Criteria Method - PGV, which leads to define a range of threats that have been divided into three groups that are human, technological and natural hazards.

Finally, this project contains several tables that detailing important information to be taken into account the most important will be those in which the application of controls is evident, and two simulations of a new local area network and a corporate network that will unify the main office with its branches, this network will be voice and data.

INDICE

Capítulo I

Tema: Introducción e información general

Evaluación de vulnerabilidades de seguridad en la empresa Booknowledge. Soluciones para mitigar las vulnerabilidades encontradas bajo la norma ISO 27001:2013.

1.2. Antecedentes.

Booknowledge es una empresa dedicada a la elaboración y venta de libros, además enfocada a cursos prácticos con metodologías y enseñanzas innovadoras.

Tiene varios años en el mercado ecuatoriano logrando hacer crecer su cartera de clientes, y conforme transcurren los años la empresa va creciendo y aumentando su personal. Actualmente cuenta con 16 empleados, divididos en 4 áreas tales como la dirección, administración, ventas y contabilidad. No existe una política de seguridad de tal manera que toda la información, contable, de clientes, de usuario etc., está disponible.

La empresa actualmente posee un servidor de correo, un portal web, gestión de archivos y facturación. Todos los empleados están conectados a la misma red incluyendo el director, es decir no está dividida o segmentada. Ninguna computadora dentro posee mecanismos de seguridad ni se han establecido los permisos de acceso a documentos por tipos de usuario dentro de la red. Por lo que se evidencia que la empresa no posee un sistema de seguridad de la información y por tal motivo es muy vulnerable y susceptible de ser atacada.

Estos factores han incitado a que se den algunos percances en la empresa como accesos indebidos a cuentas de correo de los gerentes y directores por parte de usuarios no identificados, con lo cual no se puede garantizar la confidencialidad de la información. Además, la información de base de datos no está asegurada y está comprometida de tal manera que la competencia tiene libre acceso a ella.

Es menester indicar que el área de Tics tampoco se ha preocupado en dotar a los usuarios de políticas de seguridad de la información, así como también proteger sus sistemas o configurar seguridades en los dispositivos de red y de los usuarios.

Se debe tener en consideración que la primordial política de seguridad de información es mantener la confidencialidad, disponibilidad e integridad de

esta, así como también de debe considerar que hoy en día la información de una empresa del tamaño que esta sea debe ser considerada como uno de los principales activos por el valor e importancia que esta representa.

1.3. Formulación del Problema.

Tras los antecedentes expuestos claramente se define que el problema de activos por el valor e importancia que esta representa dentro de la red de la empresa Booknowledge es muy vulnerable y ha soportado ya varios ataques del tipo interno y externo, afectando a cada unidad administrativa u operativa de la misma.

1.4. Objetivo General.

Generar una propuesta adecuada de mitigación de amenazas y ataques a la seguridad de la información para la empresa Booknowledge basada en la Norma ISO 27001:2013.

1.5. Objetivos Específicos.

Demostrar las vulnerabilidades de la red empresarial en el campo de la Seguridad de la Información.

Analizar el estado actual de la red y establecer algunas políticas necesarias de seguridad.

Investigar y dar alternativas de sistemas de seguridad en software conveniente en cuanto a presupuesto, fluidez y estabilidad.

Proponer las mejores soluciones en hardware para que se ejecuten con los mecanismos de seguridad a implementarse.

Capítulo II

2.1. Justificación del Proyecto.

2.1.1 Justificación Teórica.

Hoy en día las compañías dependen de los sistemas informáticos para realizar una determinada acción o actividad, que en ciertos casos es vital para el funcionamiento y la estructura de una empresa.

Un ataque informático puede afectar gravemente al proceso estructural de una empresa y puede generar grandes pérdidas.

Las empresas grandes generalmente tienen algún mecanismo que defiende su información como un activo más, en cambio las empresas PYMES tienen redes más vulnerables por hackers ya que descuidan este ámbito y no suelen utilizar ningún mecanismo de seguridad que pueda sustentar que la información se encuentre segura, por lo tanto, el intruso tiene más facilidad de vulnerar y atacar la red.

2.1.2. Justificación Práctica.

La propuesta de implementación de seguridad será una guía ejemplar basada en la norma ISO 27001:2013 que pueda realizar una efectiva ejecución de seguridad informática en empresas del tipo PYMES, con un presupuesto limitado y con las mejores alternativas en cuanto a estabilidad y presupuesto.

2.1.3. Norma ISA/IEC 27001.

Se enmarcará los aspectos principales de la Norma ISO/IEC 27000.

La Norma ISO/IEC 27000 “Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión” (Organización Internacional de Normalización, 2008).

Es precisamente esta definición clara de todos los conceptos la que permitirá entender el alcance que tiene la Norma ISO para el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) en una entidad o empresa.

La Norma ISO/IEC 27001 “especifica los requisitos para la implementación de un sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y

promueve la mejora continua de los procesos" (Organización Internacional de Normalización, 2008).

Como indica el texto anterior, esta norma ayuda a enfocar y solucionar los posibles riesgos que se tiene con el manejo de la información mediante sus objetivos de control y controles, también de qué manera se deben enfocar los procesos para tener la menor vulnerabilidad posible, esta norma provee una mejora continua sobre las prácticas del manejo de la información, esto es muy importante ya que en el mundo actual la evolución de la tecnología es bastante acelerada.

Estos son los puntos principales que ayudarán de manera sistematizada a organizar la situación actual en el país sobre los temas de seguridad informática.

2.1.4. Justificación Metodológica.

En el proyecto a ser desarrollado se aplicará un método deductivo ya que se comenzará analizar la red de una empresa del tipo PYME totalmente vulnerable y se aplicará una investigación de como presentar la solución de seguridad más conveniente y básicamente aplicable en el campo laboral basada en la Norma ISO/IEC 27001:2013.

2.2 Definiciones básicas y principios generales de la seguridad de la información.

2.2.1. Introducción.

En la actualidad el alto índice de crecimiento de las Tics se ha convertido en un factor delimitante a ser tomado en cuenta por las empresas o compañías ya que la información, y comunicaciones son hoy en día un activo de mucho valor. Por lo tanto, deben ser manejadas de tal manera que garanticen un alto índice de confiabilidad, integridad, y disponibilidad, para un correcto funcionamiento de las mismas.

El Internet es uno de los medios de comunicación más utilizados a nivel mundial; por lo que es la vía principal, por la cual una red estará expuesta a posibles riesgos o ataques en su integridad. En la actualidad, los virus, amenazas y ataques son muy comunes dentro de las redes; esto implica que se debe adoptar medidas que protegerán la información contenida en las mismas. (Flores & Jiménez Nuñez, 2010).

Estas políticas o normas de seguridad de la información que han sido mencionadas son un conjunto de guías o procedimientos de referencia para su implementación, y no son más que uno de los tantos métodos que existen para salvaguardar la información de una entidad.

2.2.2. Definición y necesidad de la seguridad de la información de la Vulnerabilidad.

La información puede presentarse en varias formas como se lo indico anteriormente, pero lo importante es que esta debe ser conservada y utilizada de una manera segura.

En consecuencia, la seguridad de la información hace referencia a cualquier método utilizado para proteger los datos almacenados en los dispositivos de almacenamiento contra el acceso de personas o dispositivos no autorizados. Esto es posible mediante la preservación de la Confidencialidad, Integridad, y Disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una empresa o compañía. (Flores & Jiménez Nuñez, 2010) (Villacis, 2016).

Se debe tener en cuenta que la seguridad “TOTAL” no existe ya que diariamente aparecen nuevas maneras de riesgo o amenazas, y entonces lo que se busca es reducir todos estos riesgos y amenazas a un nivel “ACEPTABLE”; por lo que este proceso debe ser mejorado continuamente. (Hernandez Pinto, 2006) (Villacis, 2016).

Una vez familiarizado con la seguridad de la información en una red corporativa o de una organización cualquiera que esta sea, es necesario mostrar la necesidad de la seguridad de la información debido a:

- Continúo desarrollo y expansión de las redes de comunicación.
- Uso de las redes de comunicaciones para transacciones en tiempo real.
- Abaratamiento de costos de equipos o software que permiten analizar los datos que circulan por la red.
- Negocios altamente dependientes de los sistemas de información y comunicación.
- El avance de la tecnología digital permite que la información sea almacenada en forma compacta y pueda ser recuperada, copiada,

transmitida o manipulada de forma rápida y clandestina. (ISO 27001 , 2013) (Villacis, 2016).

2.2.3. Retos de la Seguridad.

2.2.3.1. Confidencialidad.

Secreto del mensaje, por ningún motivo una persona no autorizada debe tener acceso a la información, incluso si es no intencional. **(Villacis, 2016)**.

2.2.3.2. Integridad.

Nadie podrá modificar la información transmitida o almacenada, es decir debe conservarse en su totalidad. **(ISO 27001 , 2013) (Villacis, 2016)**

2.2.3.3. Disponibilidad.

La información deberá estar siempre disponible y podrá ser utilizada por personas autorizadas el momento que estas lo requieran. **(Villacis, 2016) (ISO 27001 , 2013)**.

2.2.3.4. Autenticación.

La procedencia de un mensaje ha de ser completamente identificado. **(Villacis, 2016)**.

2.2.3.5. No Repudio.

Tanto emisor como receptor del mensaje no podrán negar la existencia del mismo. **(Villacis, 2016)**

2.3. Vulnerabilidades, Amenazas, Riegos y Ataques.

2.3.1. Definición de la Vulnerabilidad.

El riesgo no es más que la suma de las amenazas y vulnerabilidades encontradas o analizadas al sistema de información de una compañía o entidad. (Villacis, 2016).

La vulnerabilidad se define como la posibilidad de absorber negativamente incidencias tanto internas como externas debido a los avances de la tele comuniones, por lo que la convierte en una vía de ataque potencial. (Villacis, 2016).

El entorno de internet es un peligro constante para las organizaciones que ahora trabajan con este servicio. Los peligros más frecuentes de los que deben protegerse las empresas mientras navegan en internet son los siguientes:

- **Hackers:** También llamados piratas informáticos accedan a la información que existe y se transmite por internet, no solo tienen acceso a e-mails sino a computadoras que están enlazadas a la red perjudicando a las empresas haciendo mal uso de la información.
- **Cracker**: Son personas que intentan romper la seguridad de un sistema, accediendo con malas intenciones a la información que se mantiene guardada en ellos.
- **Virus:** Son programas diseñados para modificar o destruir datos, pueden ser ingresados al sistema por un dispositivo externo o través de la red (e-mails) sin intervención directa del atacante.
- **Gusanos:** Son virus que se activan y transmiten a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.
- **Caballos de Troya:** Son virus que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.
- **Spam:** También llamado correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y organismos.

Pero no sólo el internet es una amenaza para las organizaciones podemos encontrar otras tantas dentro de la propia empresa. Una amenaza siempre latente es el personal de la organización que por muchas circunstancias puede ser un peligro ya sea por los errores que pueda cometer sin intención como aquellos que son hechos con el objetivo de dañar a la organización un ejemplo claro es cuando en el departamento de sistemas no genera registros de las actividades de los usuarios en la red, esto provoca que no se pueda identificar anomalías que pueden realizar los empleados mientras se encuentren conectados al sistema, volviendo a la información que se genera poco confiable; si continuamos explorando dentro de la empresa podemos encontrar otras vulnerabilidades como son los equipos que no reciben el mantenimiento adecuado o que por fallas eléctricas suelen dañarse y dejar a la organización

con menos recursos para realizar sus operaciones. Las organizaciones siempre estarán expuestas a estos tipos de riesgos o ataques informáticos y a otros más ya que a medida que avanza la tecnología también habrá personas que intenten mejorar las formas de vulnerar la seguridad. (Villacis, 2016) (Hernandez Pinto, 2006).

2.3.2. Definición de la amenaza.

Es una acción o evento que puede afectar a la seguridad de un sistema de información. Tiene tres componentes que son:

- **Objetivos:** Que aspecto de la seguridad puede ser atacado.
- **Agentes:** Las personas u organizaciones que originan la amenaza.
- **Eventos:** El tipo de acción que origina la amenaza. (Villacis, 2016) (Hernandez Pinto, 2006).

Una clasificación de amenazas se encuentra en la figura 1.

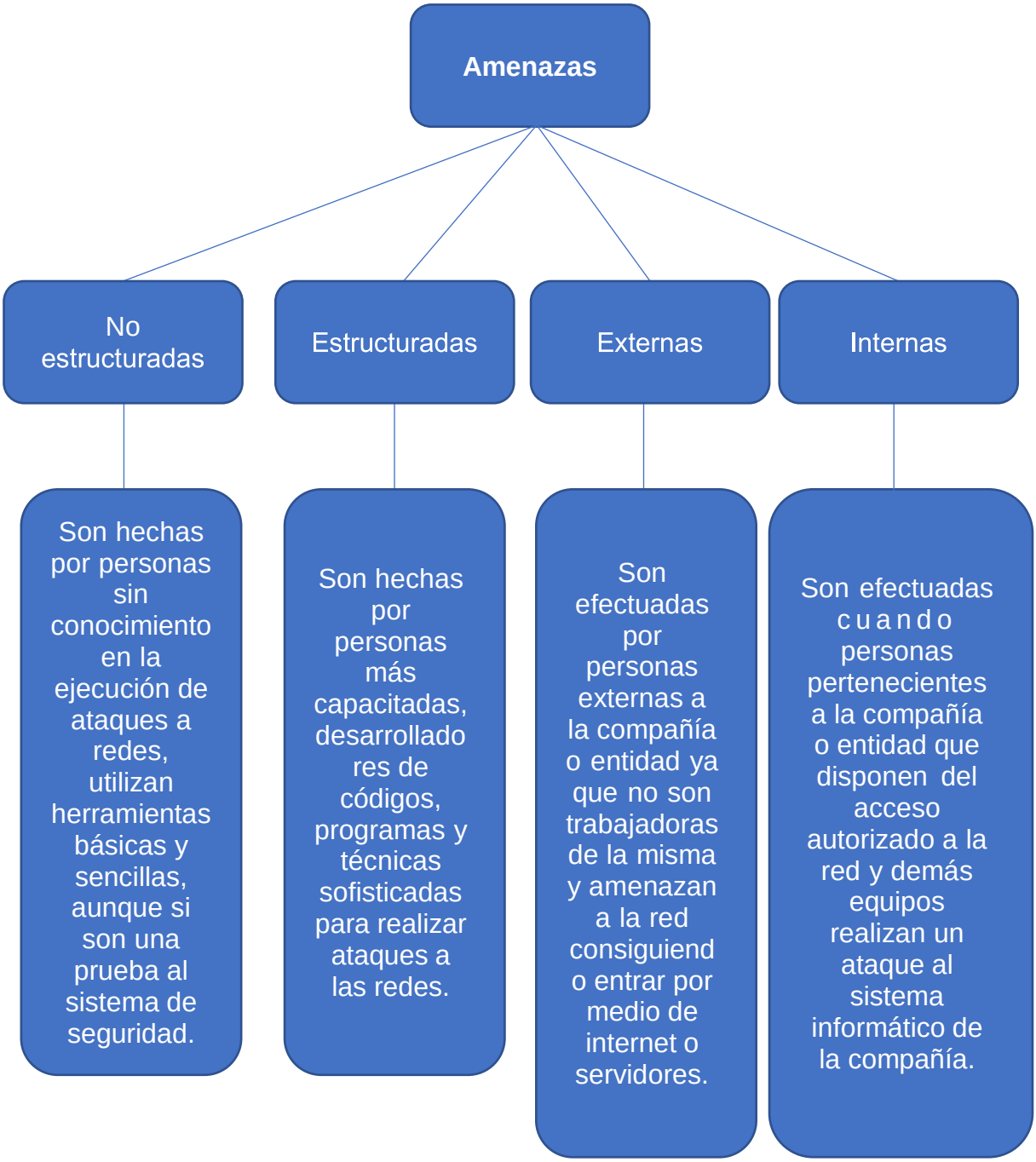


Figura # 1: Clasificación de las Amenazas.

2.3.2.1 Tipos de amenazas a la seguridad.

Ninguna empresa está dispensa de sufrir amenazas a su seguridad, estas amenazas a las que forma vulnerables las organizaciones son expuestas en la figura 2.

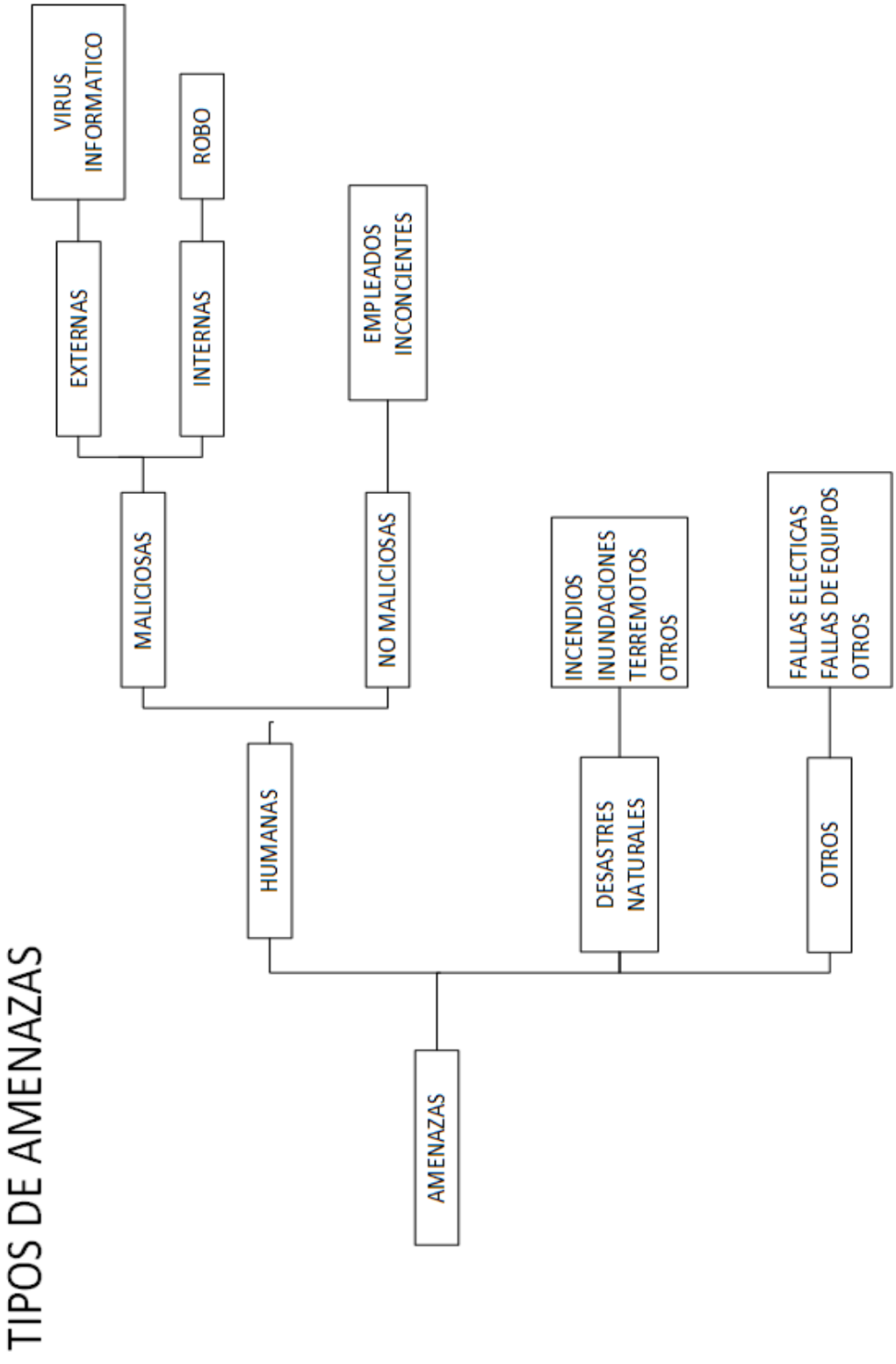


Figura # 2: Tipo de Amenazas.

2.4. Definición de Riesgo.

El riesgo no es más que la suma de las amenazas y vulnerabilidades encontradas o analizadas al sistema de información de una compañía o entidad. (Villacis, 2016) (Hernandez Pinto, 2006)

AMENAZA + VULNERABILIDAD = RIESGO

2.4.1. ¿Cómo enfrentar los riesgos?

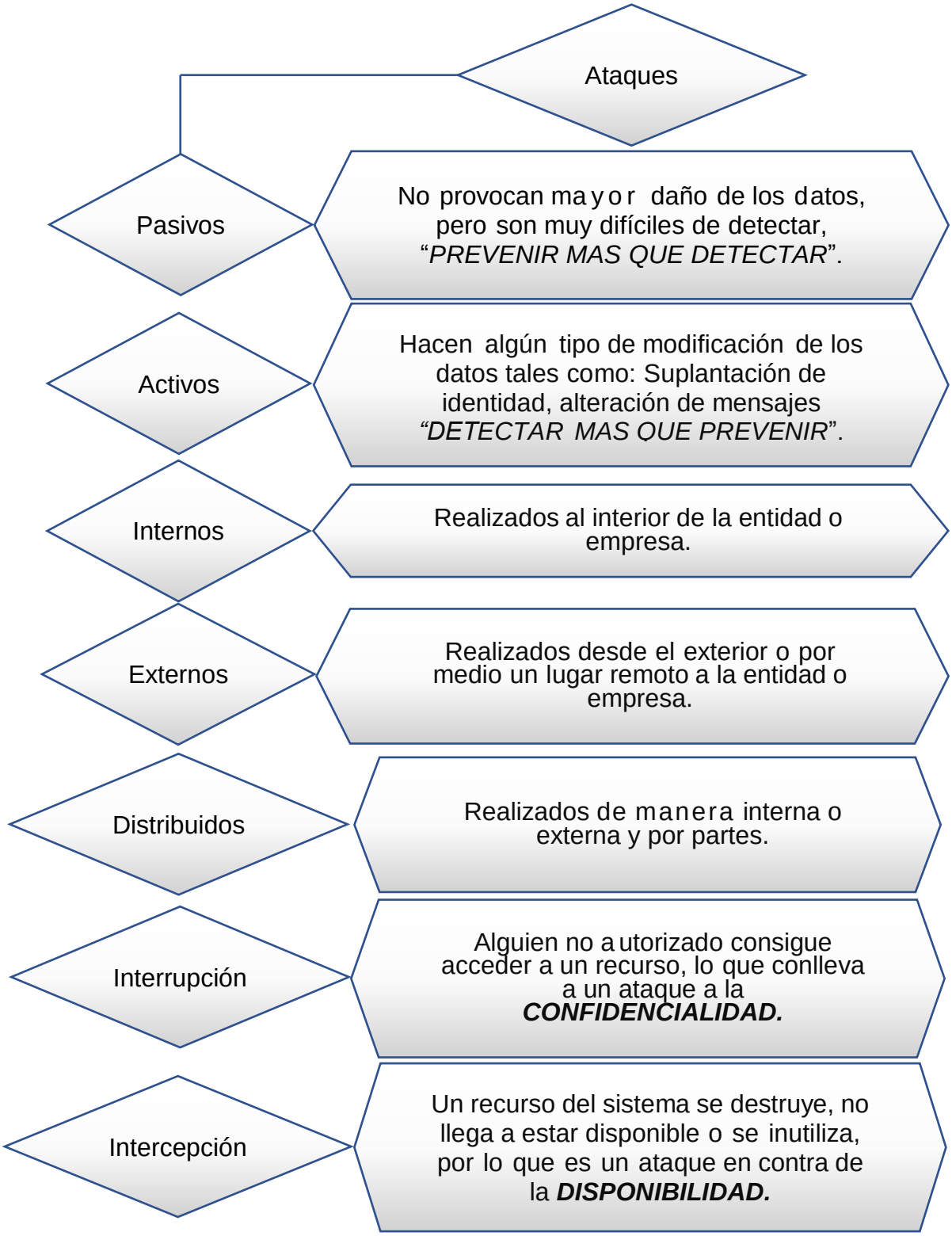
Los problemas de seguridad se duplican con gran facilidad, por lo que los mercados deben corregir los sistemas y los procesos para evadir amenazas o abordarlas cuando se produzcan. Para certificar que la información de una empresa o entidad posea las características de seguridad ya sugeridas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad informática. (Hernandez Pinto, 2006)

2.2.4. Definición de ataque.

Un ataque a un sistema informático o la seguridad de una red es la culminación de varias amenazas y vulnerabilidades realizadas por el intruso hasta que logra ingresar y causar daño al sistema, y si fuera el caso ocasionar pérdidas de información relevante a la empresa o peor aún el robo de dinero u otros activos. (Hernandez Pinto, 2006).

Se debe tomar en cuenta que los atacantes lo que quieren es conseguir documentos confidenciales, corromper la información del sistema, usar terminales remotos para la instalación de programas maliciosos, modificar el sistema operativo para causar mayores daños, robo de activos o capitales.

Clasificación de los Ataques indicados en la figura 3.



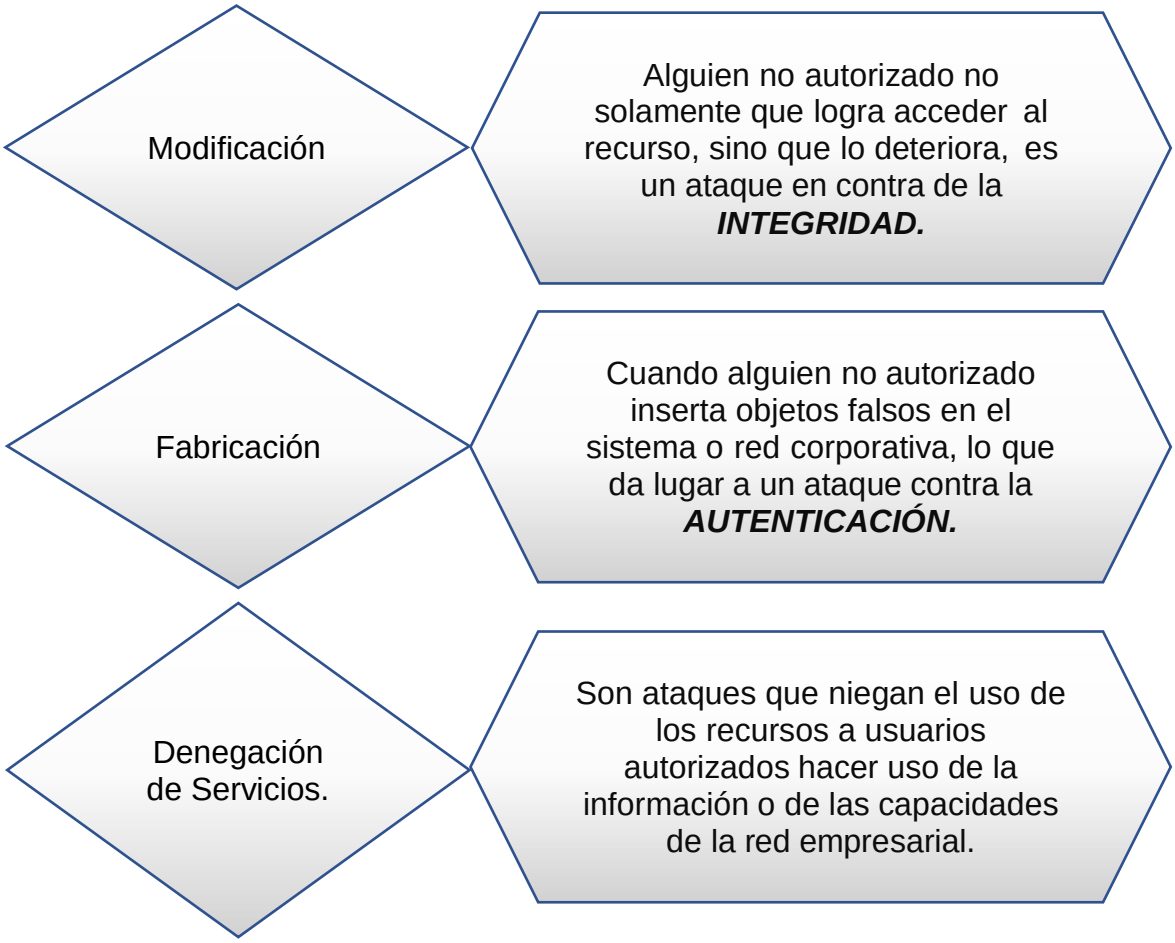
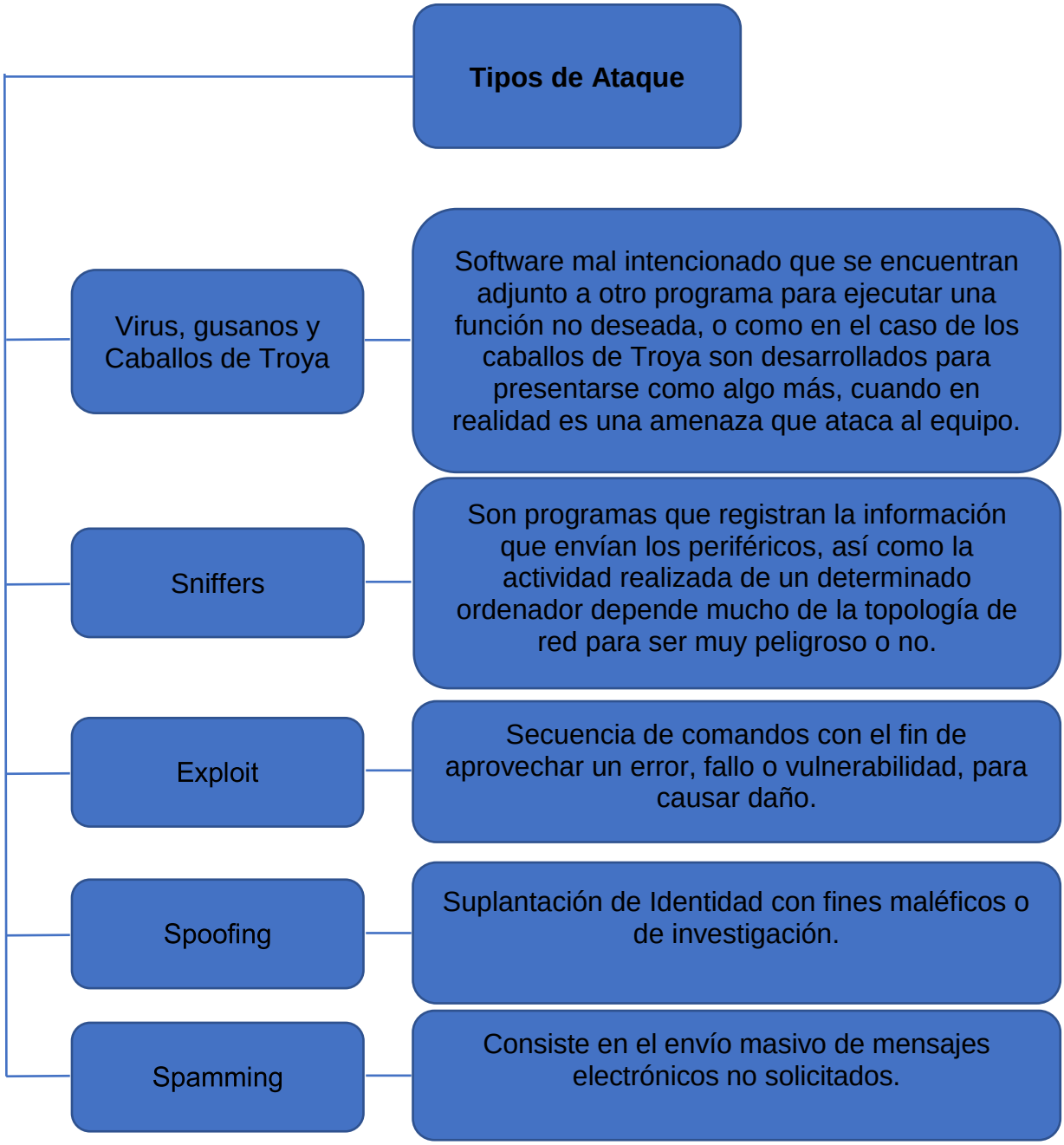


Figura # 3: Clasificación de Ataques.

2.2.4.1. Tipos de Ataques.



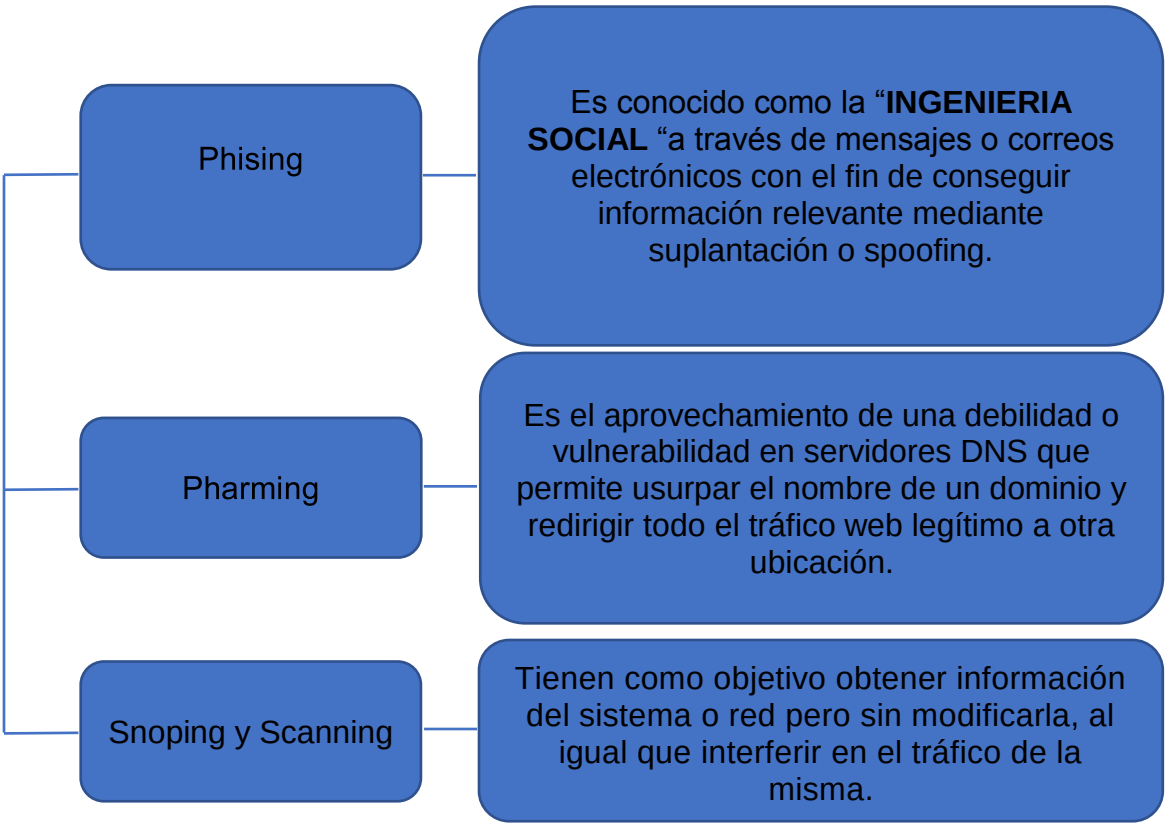


Figura 4: Tipos de Ataques.

2.2.4.2. Tipos de Atacantes.

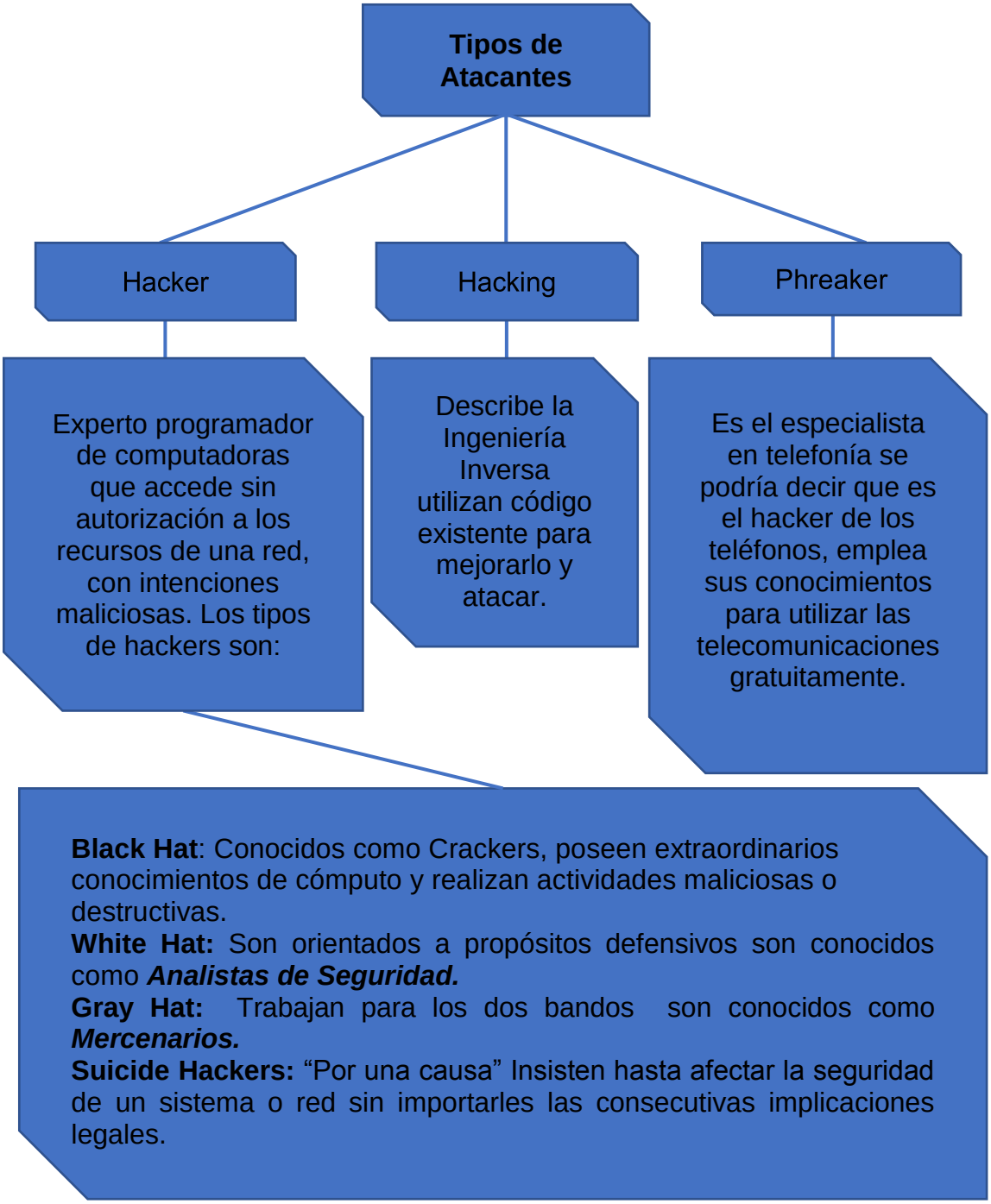


Figura 5: Tipos de Atacantes.

2.5. Historia de la ISO 27001 -2013.

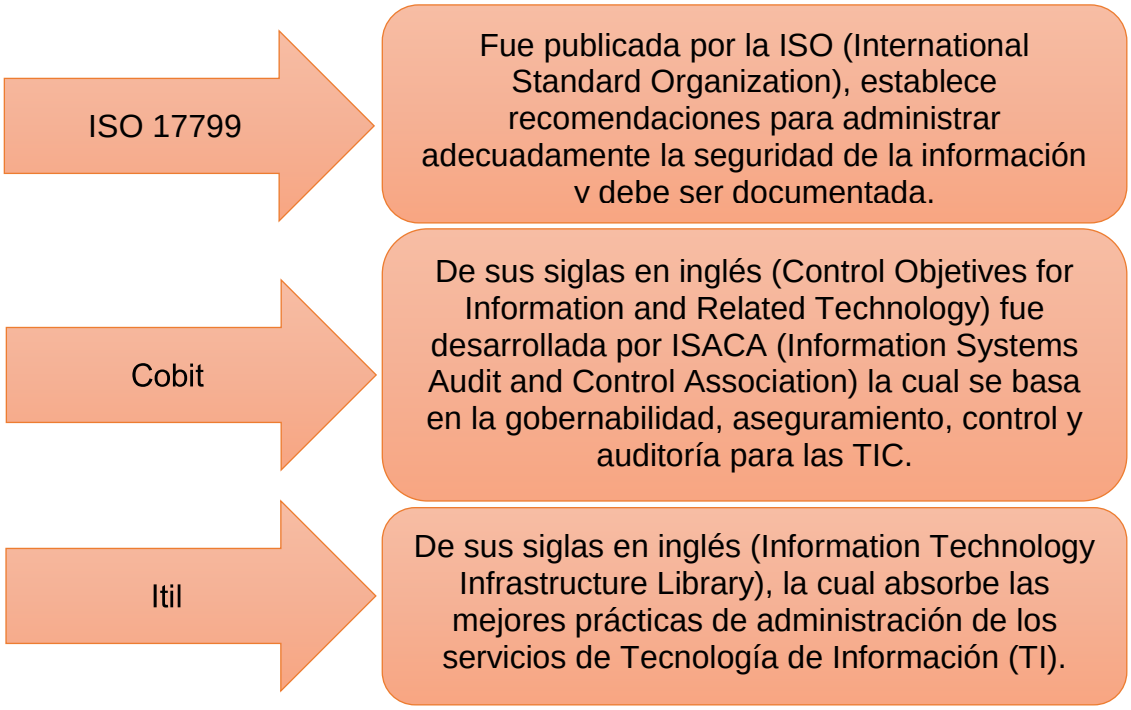
2.5. 1. Norma internacional aplicable a la seguridad de la información.

2.5.1.1. Detalle de las normas previamente publicadas.

Este estándar internacional ha sido preparado para proporcionar un modelo que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y la estructura de la organización. (ISO/IEC/JTC, 2005, pp. 4,5).

Debido a las necesidades de las entidades y organizaciones por demostrar que poseen una adecuada seguridad de la información, se han creado varias normas o estándares internacionales que permitan garantizarla entre estos los más conocidos. (Villacis, 2016)

- Normas Publicas Internacionales



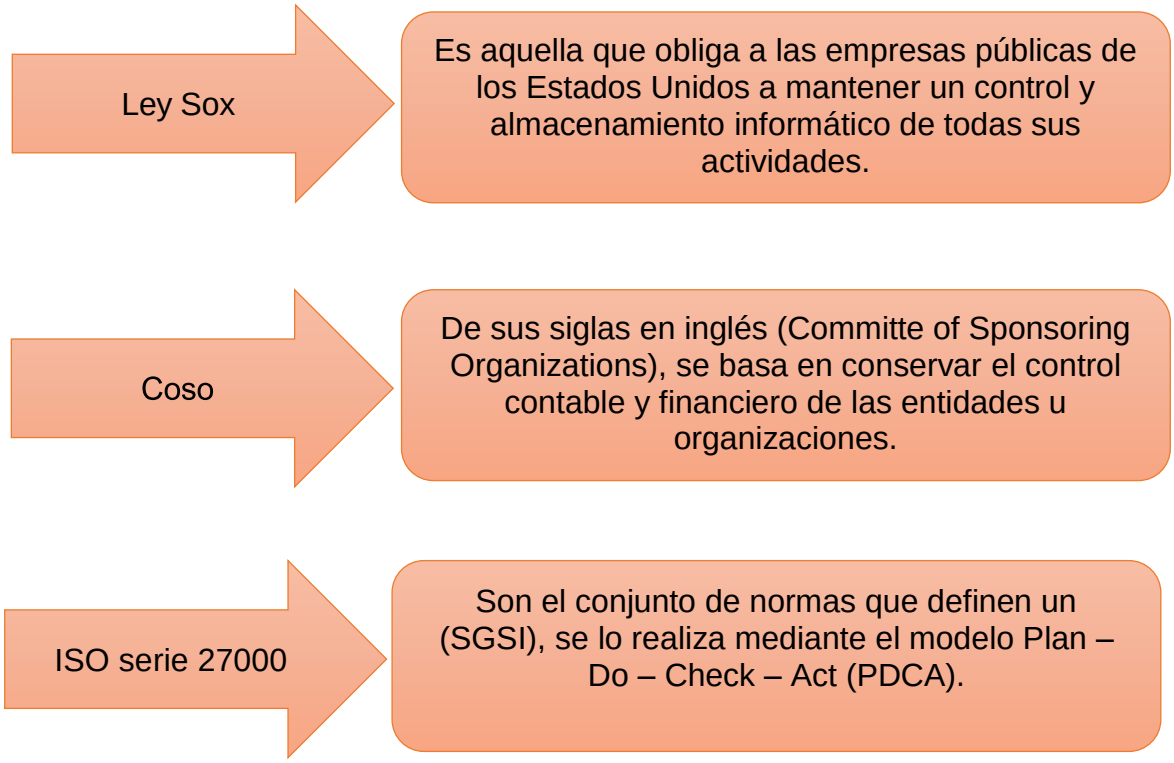


Figura 6: Normas Publicas.

2.5.1.2. Interoperabilidad entre normas.

La Interoperabilidad a través de las normas ISO como por ejemplo 9001 y la ISO serie 27000, se basa en la primera define y especifica los requisitos para administrar un sistema de gestión de calidad, mientras que la segunda detalla un SGSI (Sistema de Gestión de Seguridad de la Información). El establecimiento de un SGSI (Sistema de Gestión de Seguridad de la Información) junto con un sistema de gestión de calidad permite garantizar un servicio organizado, seguro y de mejor calidad.

La norma ISO 14001 define las especificaciones y elementos necesarios para la implementación de un sistema de gestión ambiental, un SGSI (Sistema de Gestión de Seguridad de la Información), debe procurar proveer posibles desastres naturales que pudieran afectar a la información de la empresa, además la norma considera innecesario el almacenamiento de información no actualizado, al igual que la empresa no sea necesario. Al trabajar de manera conjunta ambas normas se procurará SGSI (Sistema de Gestión de Seguridad de la Información), sea favorable al medio ambiente colaborando así con la norma ISO 14001. (Flores & Jiménez Nuñez, 2010)

2.5.2 Las normas ISO 27001.

2.5.2.1. Orígenes.

Constituyen un grupo de estándares, desarrollados por la ISO y por IEC (International electrotechnical Commission) que son generalmente conocidas como las normas ISO 27000.

Esta familia de estándares se la creo y publico bajo la necesidad de contar con una base de ejecución de la gestión de la seguridad de la información, especificando los requisitos para establecer, implementar controlar, mantener e innovar SGSI (Sistema de Gestión de Seguridad de la Información) ya que su directriz de implementación es conocido como ISMS (Information security managnent system).

La BSI (British stándar institution) desarrollo en 1995 la primera parte de la norma BS (British estándar) 7799-1 la cual proporcionaba a las empresas británicas buenos consejos y prácticas para la seguridad de su información. La BS 7799-2 fue publicada en 1998 y en ella se especifica los requisitos para un SGSI (Sistema de Gestión de Seguridad de la Información) pueda ser certificado.

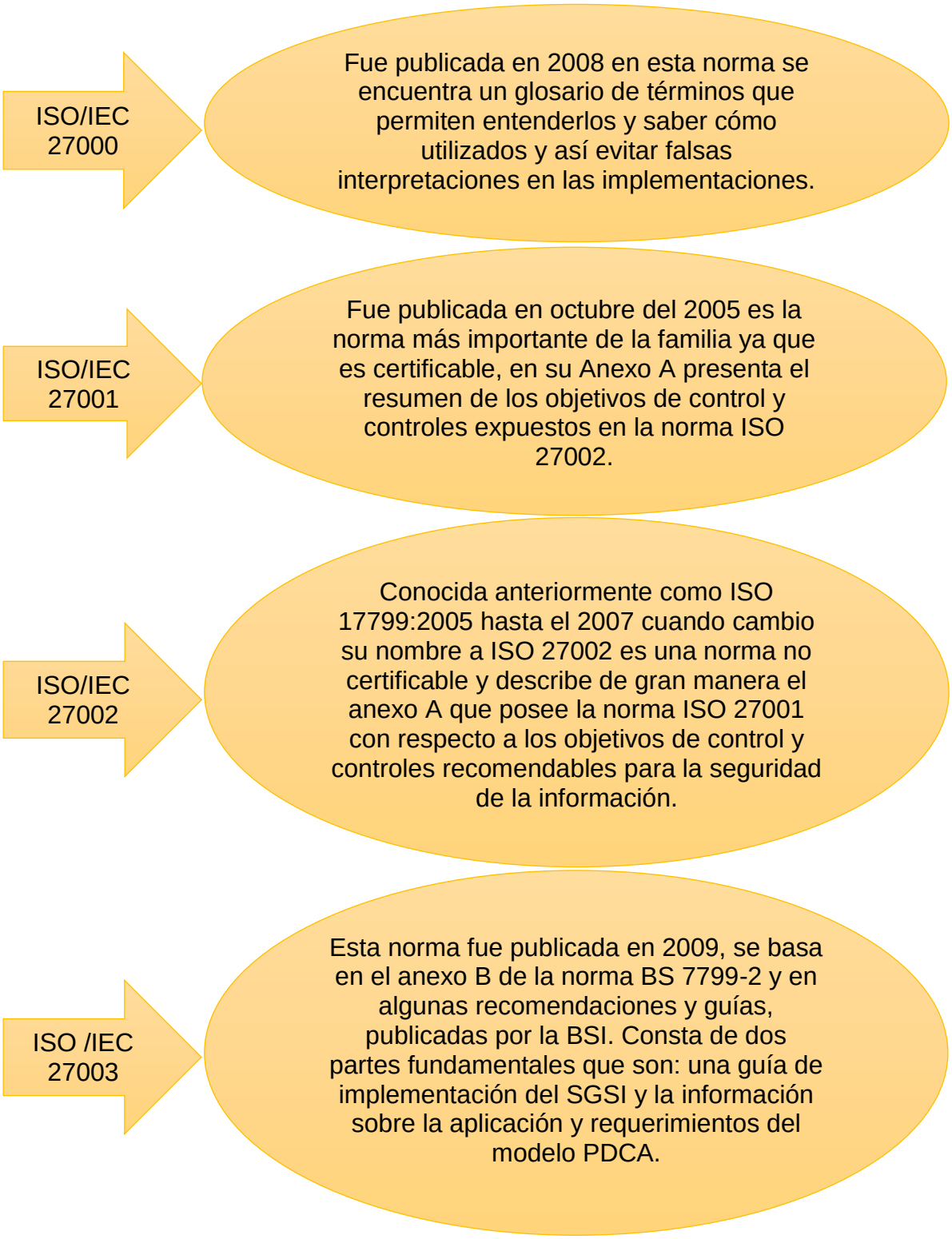
En el año 2000 la ISO adopto la norma BS 7799-1 y la denomino ISO 17799, mientras que la segunda parte de la norma fue adoptada en 2005 como ISO 27001, hasta que finalmente en el año 2007 la ISO 17799 fue nombrada como ISO 27002. Se encuentra en vigencia la norma conocida como ISO 27001:2005 con su actualización ISO 27001:2013. (ISO 27001 , 2013)

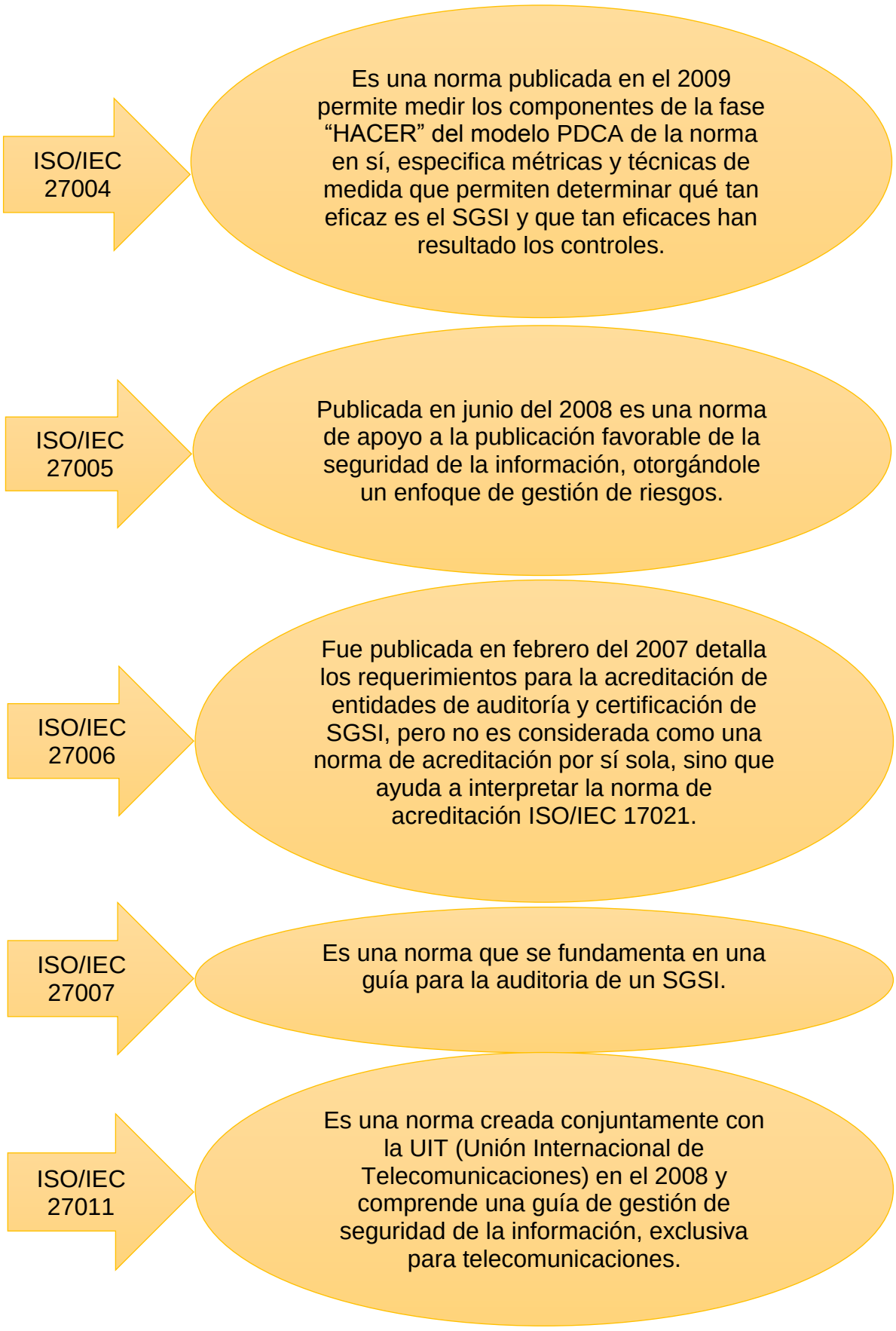
Figura #7 Historia y evolución de la ISO 27001

Adaptado de (ISO 27001 , 2013)

La figura 2 muestra la historia y evolución.

La figura # demuestra esta evolución.




ISO/IEC 27004
Es una norma publicada en el 2009 permite medir los componentes de la fase “HACER” del modelo PDCA de la norma en sí, especifica métricas y técnicas de medida que permiten determinar qué tan eficaz es el SGSI y que tan eficaces han resultado los controles.
ISO/IEC 27005
Publicada en junio del 2008 es una norma de apoyo a la publicación favorable de la seguridad de la información, otorgándole un enfoque de gestión de riesgos.
ISO/IEC 27006
Fue publicada en febrero del 2007 detalla los requerimientos para la acreditación de entidades de auditoría y certificación de SGSI, pero no es considerada como una norma de acreditación por sí sola, sino que ayuda a interpretar la norma de acreditación ISO/IEC 17021.
ISO/IEC 27007
Es una norma que se fundamenta en una guía para la auditoria de un SGSI.
ISO/IEC 27011
Es una norma creada conjuntamente con la UIT (Unión Internacional de Telecomunicaciones) en el 2008 y comprende una guía de gestión de seguridad de la información, exclusiva para telecomunicaciones.

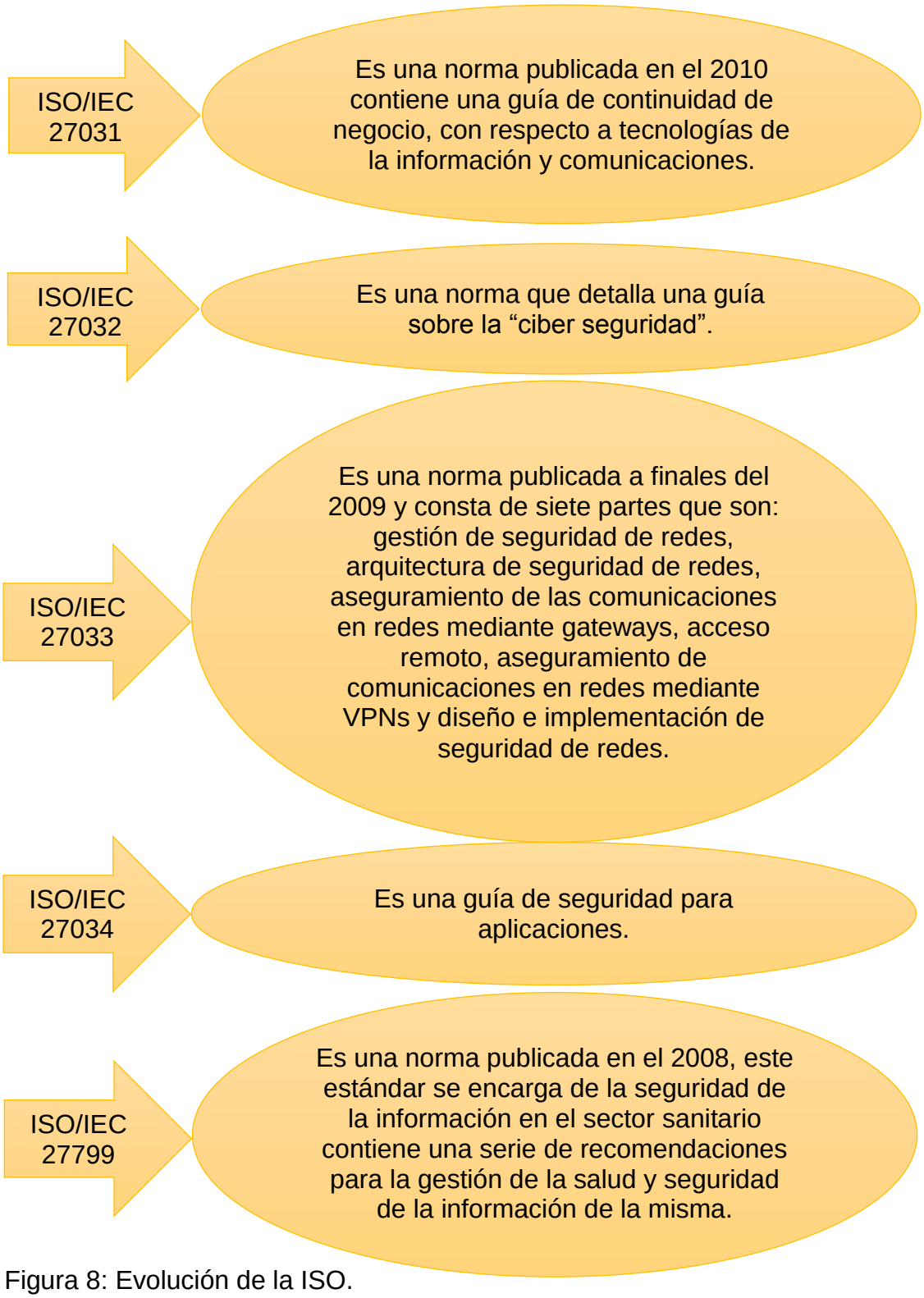


Figura 8: Evolución de la ISO.

2.5.2.2. Objetivos de la Norma.

Dentro de los objetivos de la norma ISO 27000 se tiene los siguientes:

- Contar con recomendaciones útiles para las personas encargadas de la seguridad de la información en una empresa o institución.

- Mantener y mejorar los niveles de seguridad de sistemas, redes, equipos información de la empresa o entidad, datos de los clientes, empleados, mediante la utilización de controles y analices de riesgo.
- Elaborar planes de contingencia estratégicos que ayudaran a solucionar posibles amenazas o ataque detectados al sistema, y procurando hacerlo en el menor tiempo posible de respuesta.
- Capacitar y hacer tomar conciencia al personal acerca de la importancia de la seguridad de información ya que es un activo importante de su empresa o entidad, de igual manera incentivar a que conozca sobre la norma ISO 27000.
- Elaborar y conservar una documentación de los procesos a llevarse a cabo en un SGSI (Sistema de Seguridad de la Información).
- Realizar un monitoreo y revisión constante de las recomendaciones planteadas en base la norma ISO 27000 están siendo aplicadas o si es del caso mejorarlas. (ISO 27000,2015). (ISO 27001 , 2013).

2.5.2.3. Beneficios de la Norma.

La implementación de procedimientos que garanticen la seguridad de la información presenta los siguientes beneficios.

- Se disminuye el riesgo de alteración, daño, pérdida, robo, o mal uso de la información y de esta manera se garantiza la premisa de la confidencialidad, integridad, y disponibilidad de la misma.
- Se entablan procedimientos bien diseñados, con claridad y orden que permitan una administración eficiente de la seguridad de la información.
- La integración con otras normas ISO es posible, ya que se puede tener una empresa o compañía varias normas ISO implementadas a la vez sí que interfieran una con otra.
- Ganar la confianza del personal de la empresa al garantizar seguridad y confidencialidad de la información.
- Es importante para una empresa o entidad el contar con un SGSI (Sistema de gestión de seguridad de la información) al ser un elemento diferenciador con respecto a la competencia, este factor podría ser decisivo en el mercado.

- Ganar confianza de personal de la empresa o entidad con respecto a la organización, normativa, recomendaciones y procedimientos a seguir.
- Disminuye los tiempos de fuera de servicio al presentarse un incidente.
- Simplifica el monitoreo del sistema o red que llevando a procesos que mitiguen las amenazas.
- Faculta la detención de vulnerabilidades del sistema de administración de seguridad para tomar acciones de mejora ISO 27000, 2015. (Villacis, 2016)

2.5.2.4. Evolución de la norma ISO 27000.

La norma ISO tiene una evolución con el transcurso del tiempo para ello en la figura 4 y 5 se hace referencia a este proceso evolutivo, donde se puede apreciar que la norma tiene sus inicios en los años 80 donde toma el nombre de BS779 y para el año 2005 empieza hacer denominada como la norma ISO 27001:2005 y finalmente en la actualidad se encuentra vigente la versión 2013.

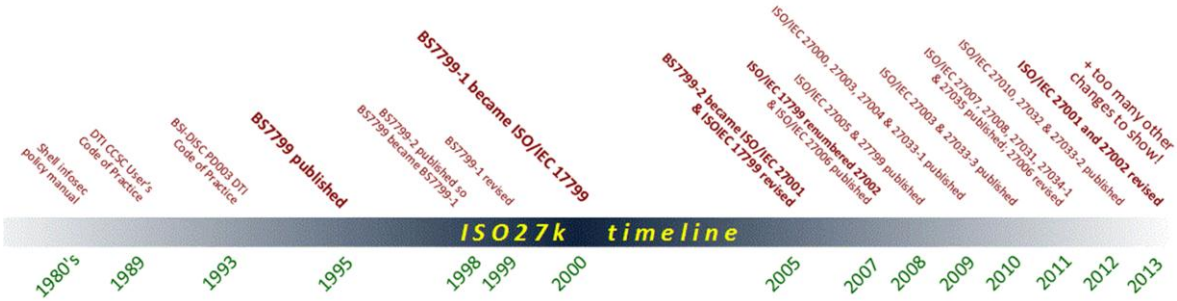


Figura # 9: Línea de tiempo de ISO 27001.
Adaptado de (ISO 27001 , 2013)

La norma ISO 270021:2013 es la única normal internacional auditable que define los requisitos para un SGSI (Sistema de gestión de seguridad de la información) y ha sido concebida para garantizar la selección de objetivos de control y controles adecuados, dependiendo cada una de las amenazas detectadas en los analices previos.

Así se asegura la protección de los activos de la información mediante un enfoque por procesos por establecer, implementar, operar, supervisar, revisar,

antener y mejorar SGSI (Sistema de gestión de seguridad de la información). (ISO 27001 , 2013).

La norma ISO 27001:2013 es adecuada para cualquier entidad u organización, del tamaño que esta sea, y es muy interesante si la protección de la información es crítica, como en finanzas, sanidad, sector público y tecnología de la información. (ISO 27001 , 2013).

El hecho de lograr avances en seguridad de la información es un gran desafío para la organización ya que no puede lograrse solo atreves de medios tecnológicos y nunca debe ser implementado de una manera que no esté alineado con el enfoque de la organización y de los riesgos encontrados o de forma tal que se creen dificultades para sus operaciones comerciales. (Flores & Jiménez Nuñez, 2010)

2.5.2.5. Introducción de los estándares ISO 27000.

En ciertas implementaciones de SGSI (Sistema de gestión de seguridad de la información) como por ejemplo el caso que compete a este proyecto de titulación es posible aplicar solo algunas normas de la familia y no todas, pues podría resultar innecesaria la implementación de toda la familia, ya que como se podrá ver en la tabla 6 del anexo 1 existen varias normas pertenecientes a este familia que se complementan entre si e incluso están en desarrollo, por esta razón la norma 27001 definirá la implementación de SGSI. (ISO 27001 , 2013)

2.5.2.6. Estándar internacional ISO/IEC 27001:2005.

Este estándar es el predecesor al estándar que se va a utilizar en este proyecto de titulación por lo que el análisis de su estructura se lo hará a continuación bajo la actualización 2013, ya que como se comprenderá son normas plenamente relacionadas. (Villacis, 2016) (Hernandez Pinto, 2006)

2.5.2.7. Introducción a la norma ISO/ 27001:2013.

Este estándar ha sido desarrollado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un

SGSI (Sistema de gestión de seguridad de la información), la adopción de un SGSI (Sistema de gestión de seguridad de la información) es una decisión estratégica por parte de una entidad o institución. Para ello el diseño e implantación del SGSI (Sistema de gestión de seguridad de la información) de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. (Villacis, 2016) (Hernandez Pinto, 2006).

El enfoque de este proceso en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para ella.
- Implementar y operar controles para reducir los riesgos de la seguridad de la información.
- Monitorear y revisar y desempeño y la efectividad del SGSI (Sistema de gestión de seguridad de la información).
- Proponer un mejoramiento continuo en base a la medición del objetivo. (ISO 27001 , 2013).

Para ello en la figura 9 se esquematiza el impacto de los riesgos en una organización evidenciándose la necesidad de implementar SGSI.

Figura # 10: Impacto de Riesgos.

Adaptado de (Villacis, 2016)

El estándar internacional que se está tratando adopta el modelo de proceso PDCA (Planear-Hacer-Chequear-Actuar), el mismo que toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y atreves de las acciones y procesos necesario produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas (Villacis, 2016) (Hernandez Pinto, 2006).

La figura 10 muestra el esquema de la normal adoptada con su modelo de procesos PDCA (Planear-Hacer-Chequear-Actuar).

Modelo PDCA

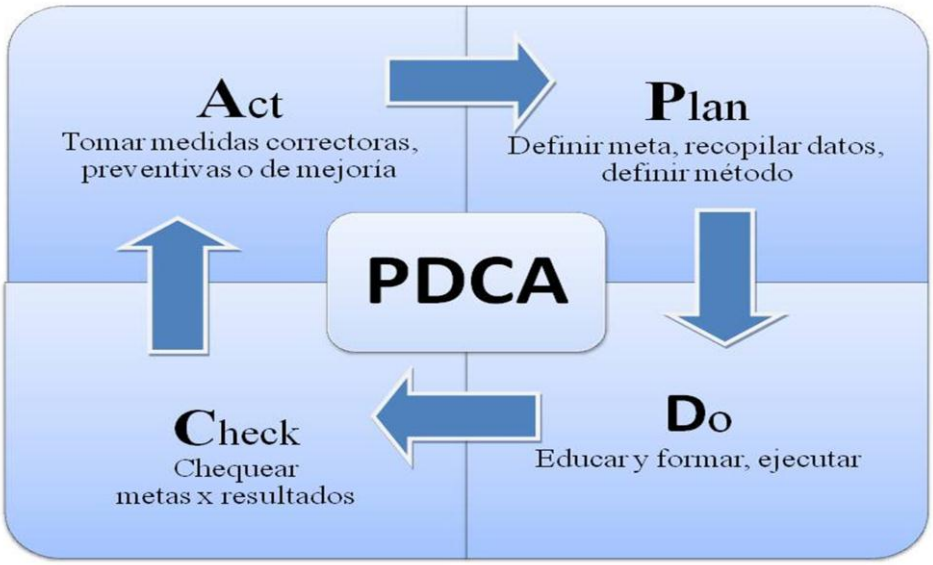


Figura #11: Modelo PDCA.
Adaptado de (Villacis, 2016)

Cabe mencionar que este estándar se puede aplicar en todos los tipos de organizaciones como empresas comerciales agencias gubernamentales, organizaciones sin fines de lucro, etc. (Villacis, 2016) (ISO 27001 , 2013).

A esto se contrapone el ciclo PDCA (Planear-Hacer-Chequear-Actuar) de la norma ISO 27001:2005 y el nuevo ciclo PDCA (Planear-Hacer-Chequear-Actuar) de la norma ISO 27001:2013, en donde claramente se evidencia la actualización de una versión a otra pero que en su contexto buscan el mismo fin. De igual manera para una mejor visualización del proceso evolutivo de la norma ISO 27001:2005 a la norma ISO 27001:2013, estas diferencias básicamente son que se eliminan los anexos B y C de la norma 2005, al igual que algunos títulos de los contenidos han sido cambiados, esto se evidencia en la versión 2013 debido a que aparecen criterios de la organización, liderazgo, planificación, soporte, operaciones, etc. (Villacis, 2016) (Hernandez Pinto, 2006).

De igual manera se puede evidenciar las diferencias en anexo A de cada norma, las principales diferencias son el número de objetivos de control ya que para cada versión 2005 se tiene 11 mientras que para versión 2013 se tiene 14, cabe mencionar que este anexo es de suma importancia ya que es el conjunto

de objetos de control y controles que norma propone para mitigar las amenazas. (Villacis, 2016).

Contraposición de los siglos PDCA de las Normas 2005 y 2013.

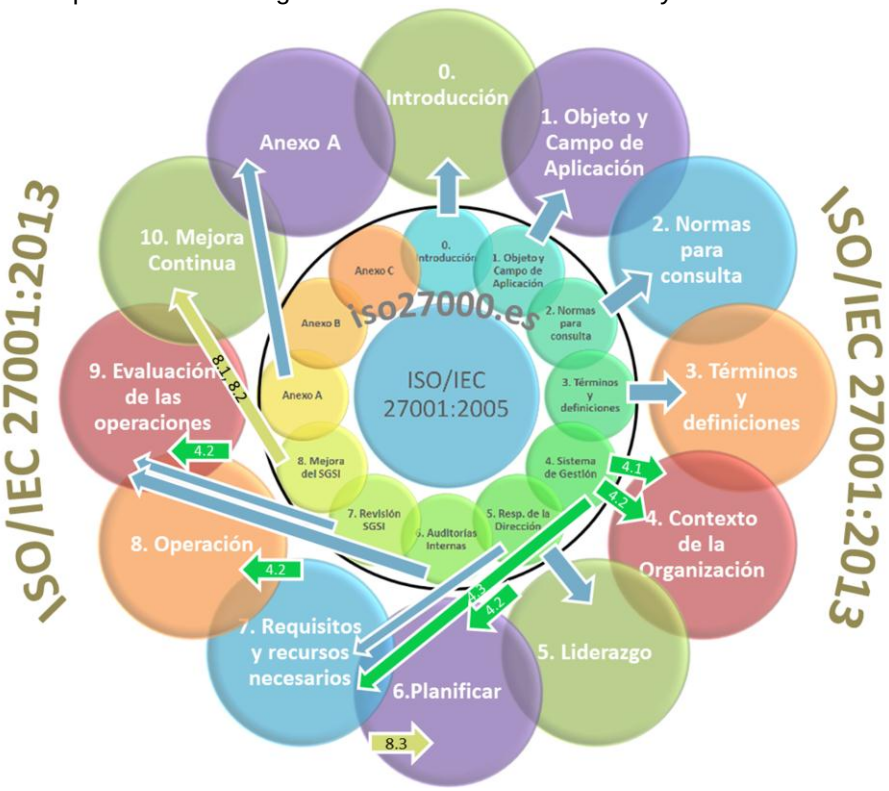


Figura #12. Contraposicion de PDCA.
Adaptado de (Villacis, 2016)

2.5.3. Modelo PDCA (Planear – Hacer – Chequear - Actuar) aplicado a los procesos SGSI.

Los procesos se gestionan mediante una técnica llamada PDCA (Planificar, Hacer, Verificar y Actuar), cada una de estas iniciales corresponde a las 4 fases de gestión del proceso, este ciclo es más usado para implantar un sistema de mejora continua.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de insumos en output (volumen de producción o salida de una empresa), se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el insumo del siguiente proceso.

Modelo PDCA aplicado a los procesos SGSI.

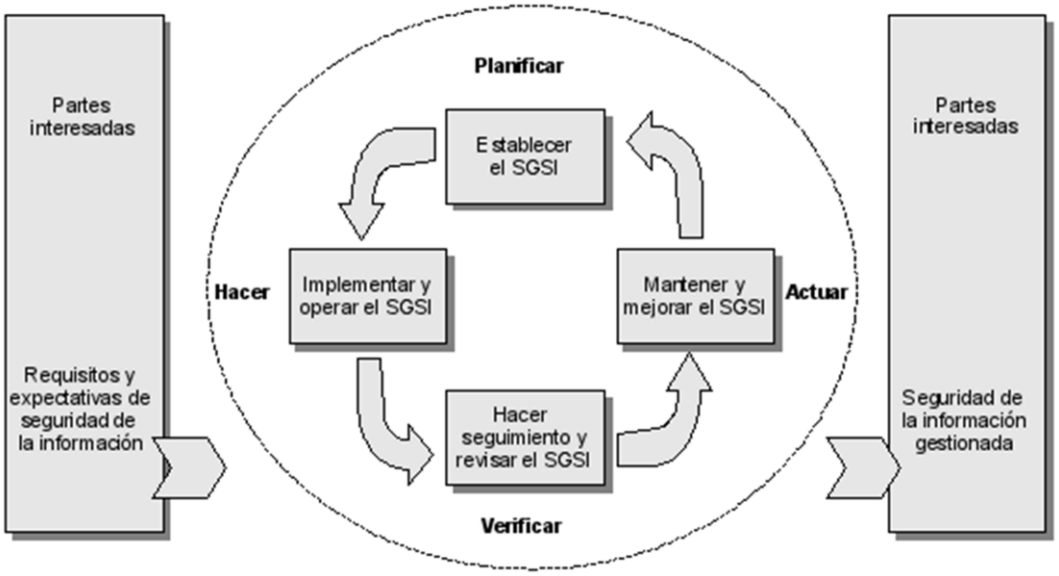


Figura #13 Modelo PDCA.
Adaptado de ISO/IEC/JTC/2015.

ISO 27001, adopta el modelo del proceso Planear – Hacer – Chequear – Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La figura 6 muestra cómo un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. (ISO 27001 , 2013) (Villacis, 2016).

2.5.4. Planeación para la implementación de un Sistema SGSI.

Utilice este ciclo para mejoramiento continuo de procesos, este modelo es muy usado para la implementación de sistemas de Gestión, en este caso un Sistema de Gestión de Seguridad de la información, ya que permite una efectiva organización y documentación, lo cual es requerido en este proceso.

Estrategia implementada en cuatro pasos detallados a continuación.

Modelo PDCA

Figura #14: Modelo PDCA-SGSI.
Adaptado de (Villacis, 2016)

2.5.5. Planificar.

Incluye determinadas metas, objetivos y determina términos para alcanzar las metas estas son:

- Definiciones políticas y Objetivos
- Determinación de alcance
- Valoración de activos
- Analisis de riesgos
- Gestionar los riegos
- Seleccionar los controles ISO 17799:2005.

2.5.6. Hacer.

Incluye asegurar la educación y el entrenamiento e implementar el trabajo estas son:

- Definir e Implementar Plan de Gestión de Riesgo.
- Implementar Controles Seleccionados y sus Indicadores.
- Implementar el Sistema de Gestión.

2.5.7. Actuar.

- Identificar e implementar las mejoras.
- Adoptar acciones correctivas y preventivas.
- Verificar que las mejoras cumplan su objetivo. (Villacis, 2016)

Capítulo III

3.1. Situación actual de la empresa Booknowledge.

En la actualidad la gran evolución de las empresas privadas, ha llevado a las organizaciones a prepararse con medios y herramientas de gran importancia empresarial para justificar y cumplir con todas las demandas y necesidades exigidas por los clientes, para lo cual la elaboración del plan estratégico y es fuente clave para el desarrollo eficiente de la organización.

El proyecto propuesto tiene como objeto principal el fortalecer las vulnerabilidades de la red, anular las amenazas, riesgos, ataques informáticos perjudicando a la información de la empresa, aprovechar las oportunidades y fortalezas mostradas por la empresa mediante el SGSI. Que permitirá identificar los puntos críticos que requieren los planes de acción inmediato, debido a su impacto en la organización.

Basado en este análisis se buscarán respuestas a los principales problemas de la empresa Booknowledge, a través de la elaboración de proyectos de mejoramiento que permitan soluciones, generando un beneficio para la empresa reflejado en ahorro de recursos, tato económico como material.

Actualmente la empresa Booknowledge no cuenta con dispositivos que permitan bloquear o contrarrestar las posibles amenazas a la información sean estas internas como externas ya que como se menciona en los antecedentes se han venido presentando diversos problemas por ataques de Hackers, Malware, Virus, Troyanos, etc. Que han afectado la integridad, disponibilidad y la confidencialidad de algunos usuarios y de la compañía.

Con lo antes expuesto durante un periodo de estudio de 90 días se han detectado varios tipos de amenazas.

3.1.1. Amenazas humanas:

Provocadas por el factor humano y pueden ser de dos tipos maliciosas y no maliciosas.

- **Maliciosas:** Son aquellas que se llevan a efecto con el propósito de causar daño a la organización.
- **No maliciosas:** Producidas en la mayoría de los casos por errores ocasionados por los usuarios que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas.

3.1.2. Amenazas externas:

Que pueden afectar al desarrollo y buen funcionamiento de las actividades de las empresas y frecuentemente son originadas por el acceso a internet, ya que en esta red existen una serie de peligros como son los virus, hackers entre otros; que infiltrándose en la red interna de la organización provocan daños como mal funcionamiento de los sistemas y pérdida de información.

3.1.3. Amenazas internas:

Más frecuentes son las originadas por los propios funcionarios y exfuncionarios de la organización motivados por la falta de dinero o represalia por algún tipo de enfrentamiento que hayan tenido con un superior.

3.1.4. Amenazas por desastres naturales:

Estas amenazas originadas por la naturaleza son las menos frecuentes en las organizaciones, pero aun así no podemos dejar de considerarlas.

Se debe recalcar que actualmente la red de la empresa Booknowledge posee poca seguridad debido a que toda la conexión hacia/desde internet proviene directamente desde un Modem ADSL provisto por el proveedor de servicio, con lo que es indispensable la implementación de seguridades.

3.2. Generalidades de la empresa.

En el año de 1985 la empresaria colombiana Lorena Paola Ganchala Chiriboga llega a la ciudad de Quito-Ecuador con el fin de asesorar e impulsar el arte y la lectura, fundando la empresa de libros Booknowledge. Tras años de fructífera labor y experiencia abre en el año de 2001 en la ciudad de Miami,

Florida una oficina ofreciendo exposiciones, libros de su autoría, galerías de arte y arquitectura urbana, fundando Booknowledge.

En la actualidad Booknowledge, es una empresa en constante desarrollo que ofrece varios servicios de arte y cultura en el país, tiene su oficina matriz en la ciudad de Quito, cabe mencionar que en la actualidad la presidencia de la misma se encuentra en manos de la tercera generación de la familia Ganchala.

Booknowledge, tiene su principal desempeño en el arte de la lectura, no obstante, el compromiso de mejora continua ha impulsado la oferta de servicios para el mercado investigativo y cultural.

3.3. Topología de la red existente.

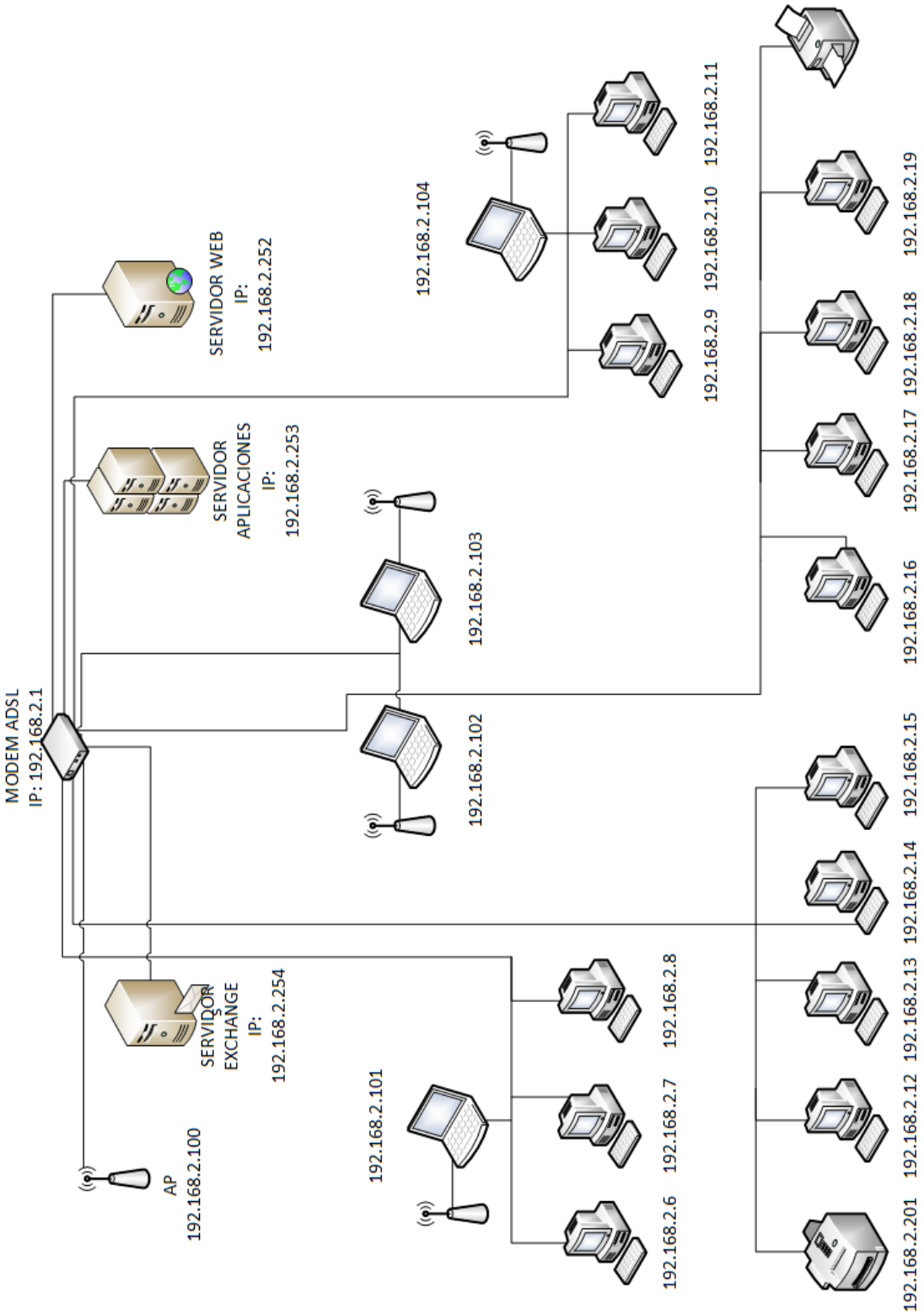


Figura # 15: Topología de la red.

3.4 Adaptación de la Norma ISO/IEC 27000 -2013.

En ciertas ejecuciones de SGSI como por ejemplo el caso que pertenece a este proyecto de titulación es viable emplear solo algunas normas de la familia y no todas, pues podría implicar innecesaria la implementación de toda la familia, existen varias normas pertenecientes a esta familia que se complementan entre sí e incluso están en desarrollo, por esta razón la norma 27001 es quien concretará la implementación de un SGSI ya que es la única certificable.

Pasos para implementar o Adaptar ISO 27001 a Booknowledge

- Utilizar metodología para gestión de proyectos.
- Definir el alcance de SGI.
- Redactar políticas de seguridad de la información.
- Definir la metodología de evaluación de riesgos.
- Realizar la evaluación y el tratamiento de riesgos.
- Redactar la Declaración de aplicabilidad.
- Redactar el Plan de tratamiento de riesgos.
- Definir la forma de medir la efectividad de los controles y del SGSI.
- Implementar todos los controles y procedimientos necesarios.
- Realizar todas las operaciones diarias establecidas en la documentación del SGSI.
- Implementar programas de capacitación y concienciación.
- Monitorear y medir el SGSI.
- Realizar la auditoría interna.
- Realizar la revisión por parte de la dirección.
- Implementar medidas correctivas.

3.5. Análisis de vulnerabilidades y ataque de la empresa Booknowledge.

3.5.1. Pruebas técnicas.

Se realiza análisis con la Herramienta Nessus v6.10 encontrando que los servicios como el SSL que no están actualizados en el sitio web y un atacante podría ejecutar código remotamente, se anexa imágenes de las pruebas.

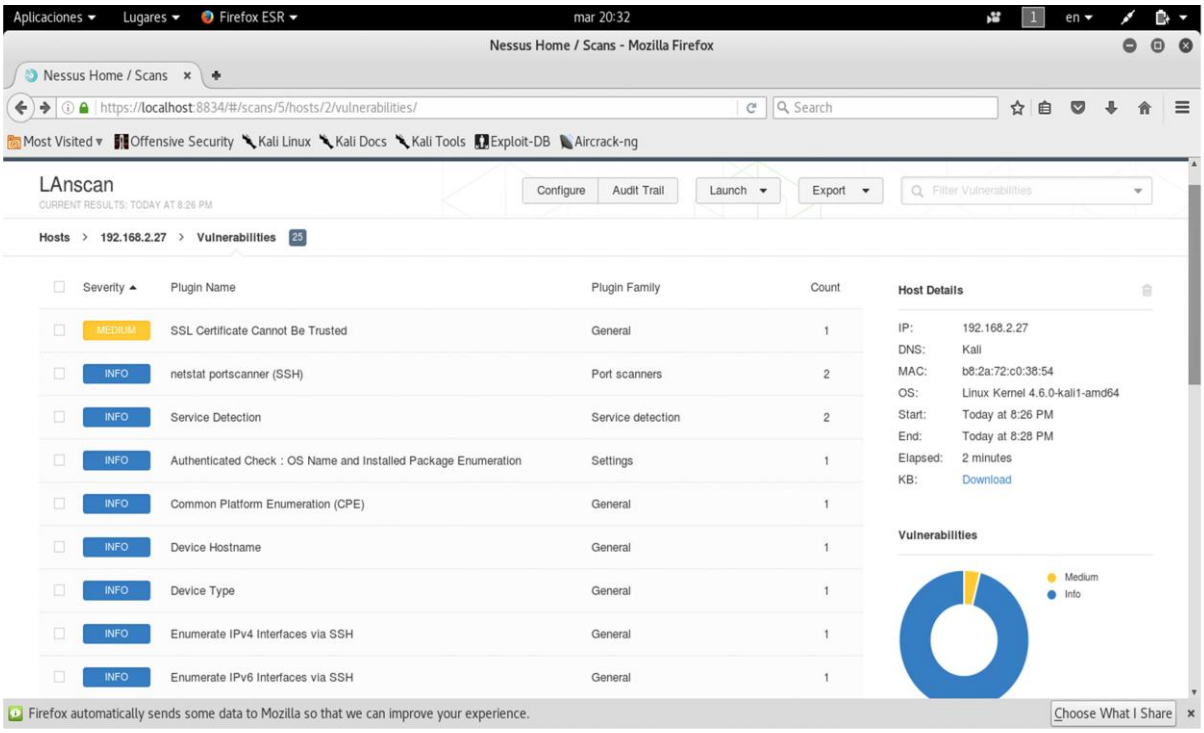


Figura #16: Análisis de LAN con NESSUS.

- También se encuentra el servidor web en una versión muy desactualizada que permite hacer exploits y tomar el control del servidor con un usuario administrador.

- Se realiza análisis al sitio web www.booknowledge.com, se encuentra que existe acceso libre hacia los archivos index.php y otros, con lo cual un hacker puede fácilmente hacer inyección de código.

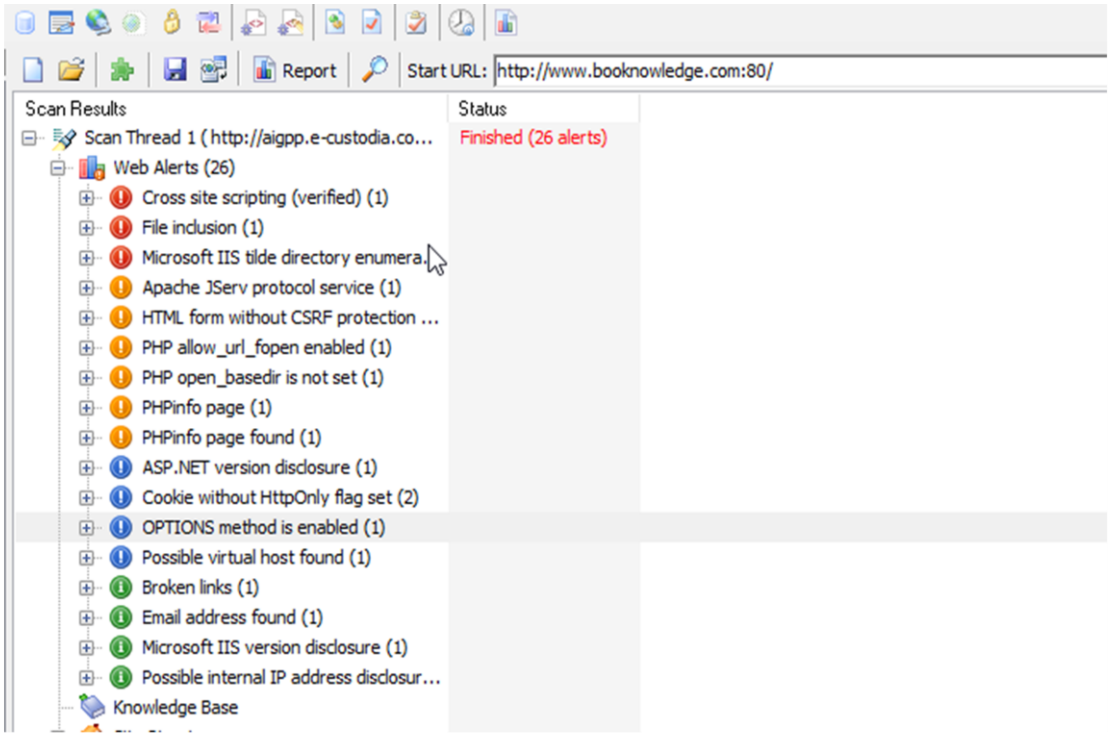


Figura # 17: Análisis de sitio web.

clientes/g2g/aplBannerClickG.php?ori=Tourism&Services_page&tema=img_isabelall&des=http://www.go2galapagos.com/luxuri_yacht.htm	404
clientes/g2g/aplBannerClickG.php?ori=hotels_page&tema=img_unihotel_featured&des=http://www.go2galapagos.com/mini_pages/HOTELUNIP..	404
portafolio	404
38-servicios/116-e-custodia	404
username-reminder-request	404
soporte/msn/index.html	404
soluciones_web/mantenimientoWeb.html	404
38-servicios	404
el_blog/entradas.php?id=3	404
seguridad_web/	404
blog/9-el-rosado-retail	404
el_blog/index.php?pageNum_entradas=2&totalRows_entradas=32	404
38-servicios/118-stupendo	404
unete/19-carousel	404
39-diferencia	404
clientes/g2g/aplBannerClickG.php?ori=hotels_page&tema=go2_unihotel_featured&des=http://www.go2galapagos.com/mini_pages/HOTELUNIP..	404
servicios/38-servicios/118-e-billing-retail	404
el_blog/entradas.php?id=73	404
38-servicios/118-e-billing-retail	404
sala-prensa/en-medios/159-facturacion-ecuador	404
servicios/38-servicios/116-e-custodia	404
servicios/38-servicios/117-facturabox	404
26-equipo/42-pponce	404
26-equipo/41-hbock	404
alfresco/index.html	404

Figura # 18: Análisis de sitio web 2.

- Se encuentra que no existe control de acceso de usuarios mediante un

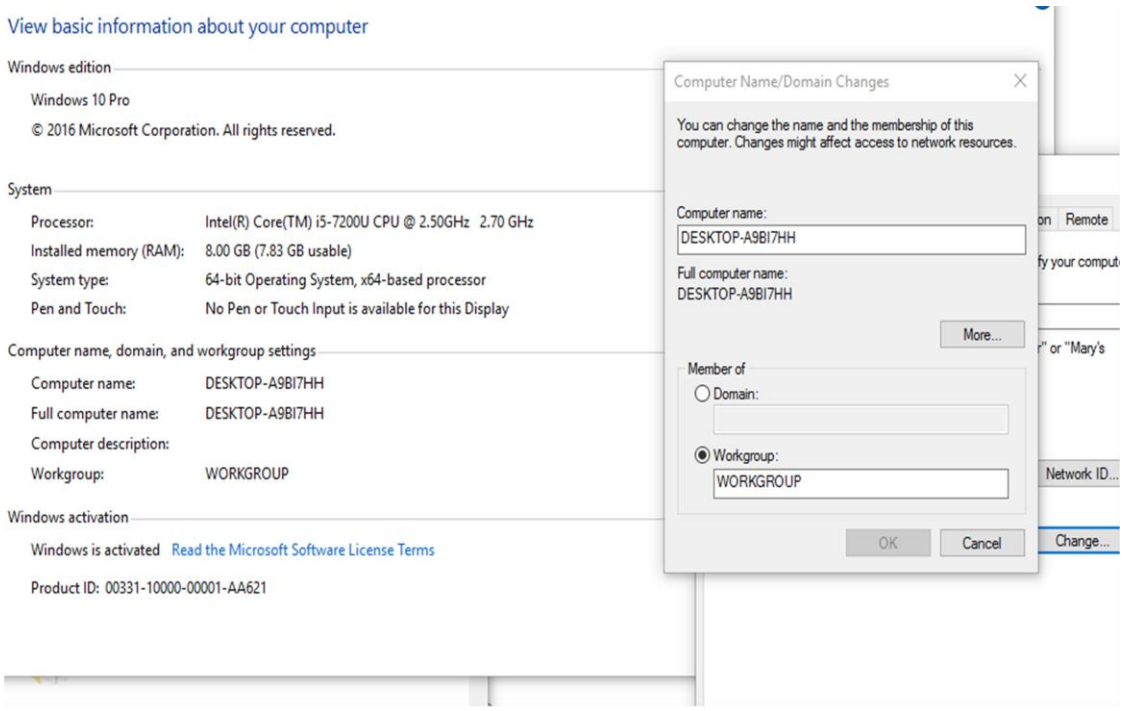


Figura #19: Active Directory.

- Se realiza Scanner a toda la red para detectar las vulnerabilidades.

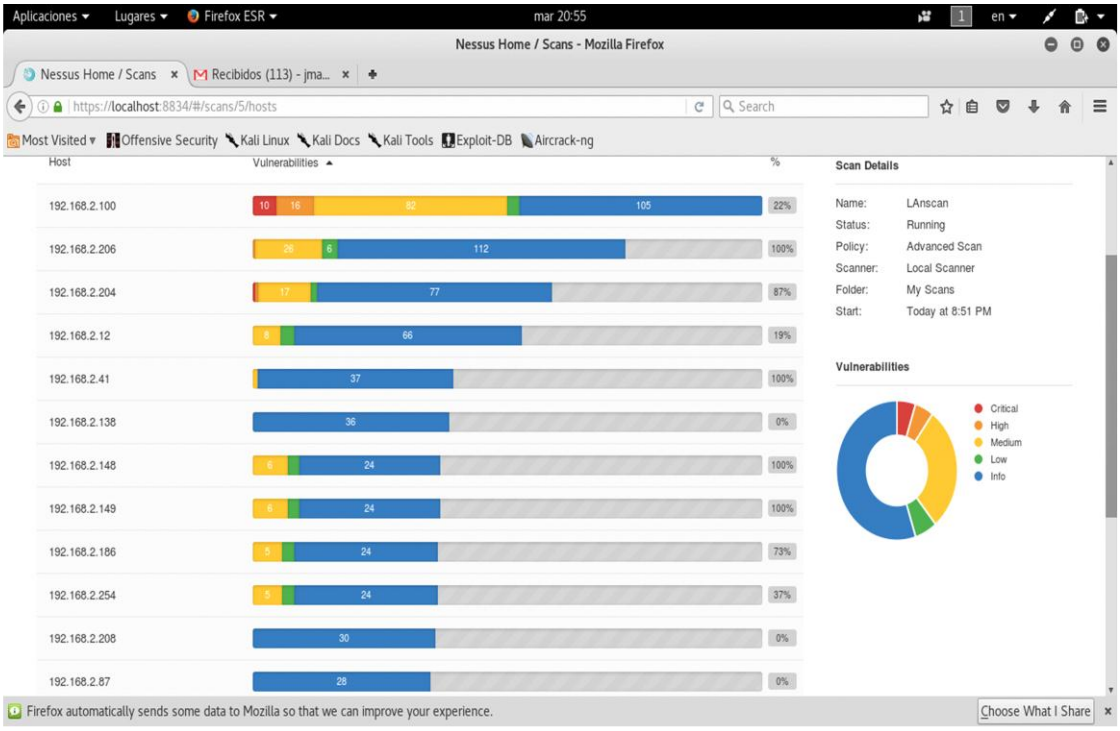
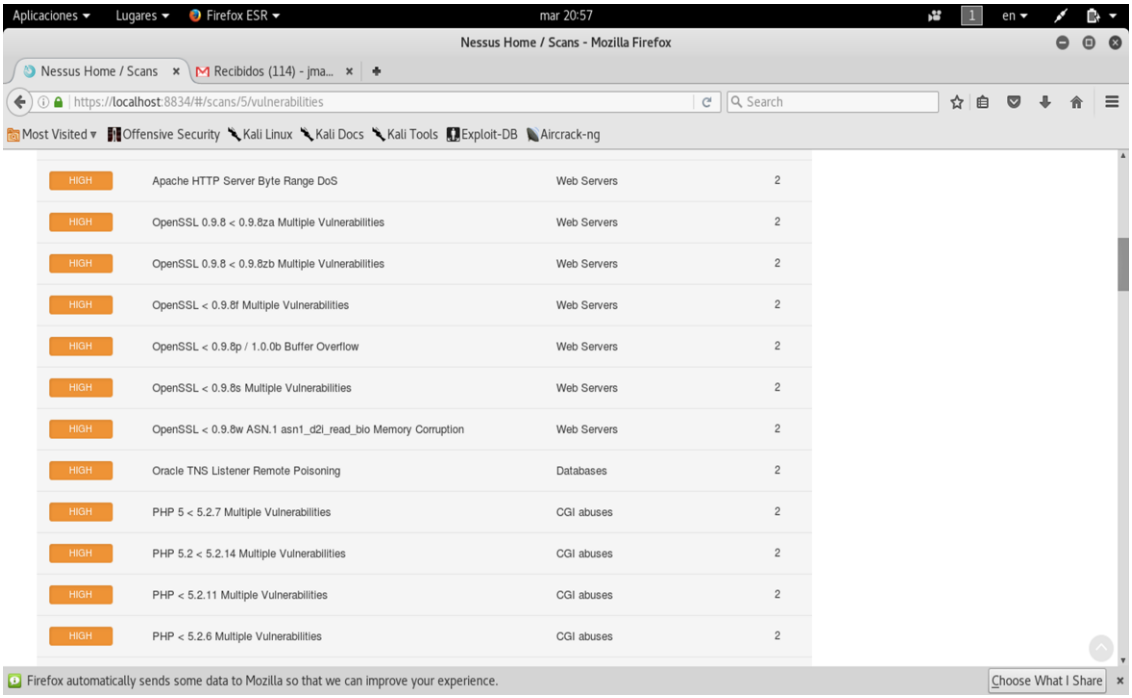
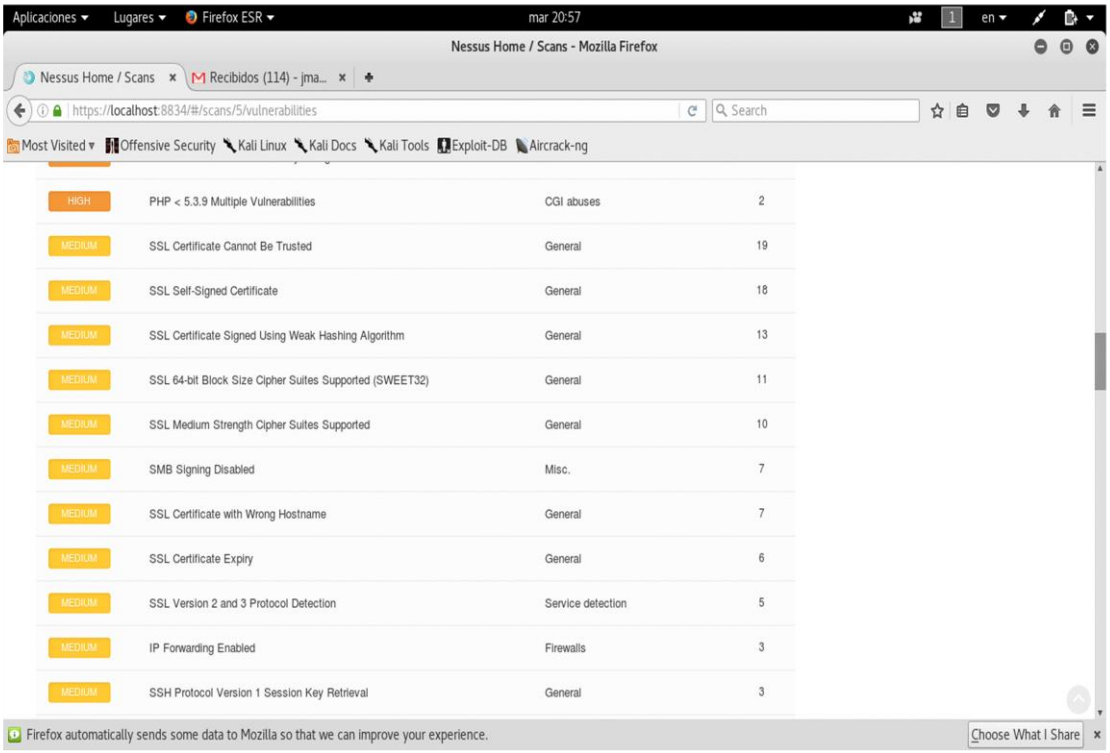


Figura #20: Análisis total de red.

Resultado de Scanner de Vulnerabilidades.





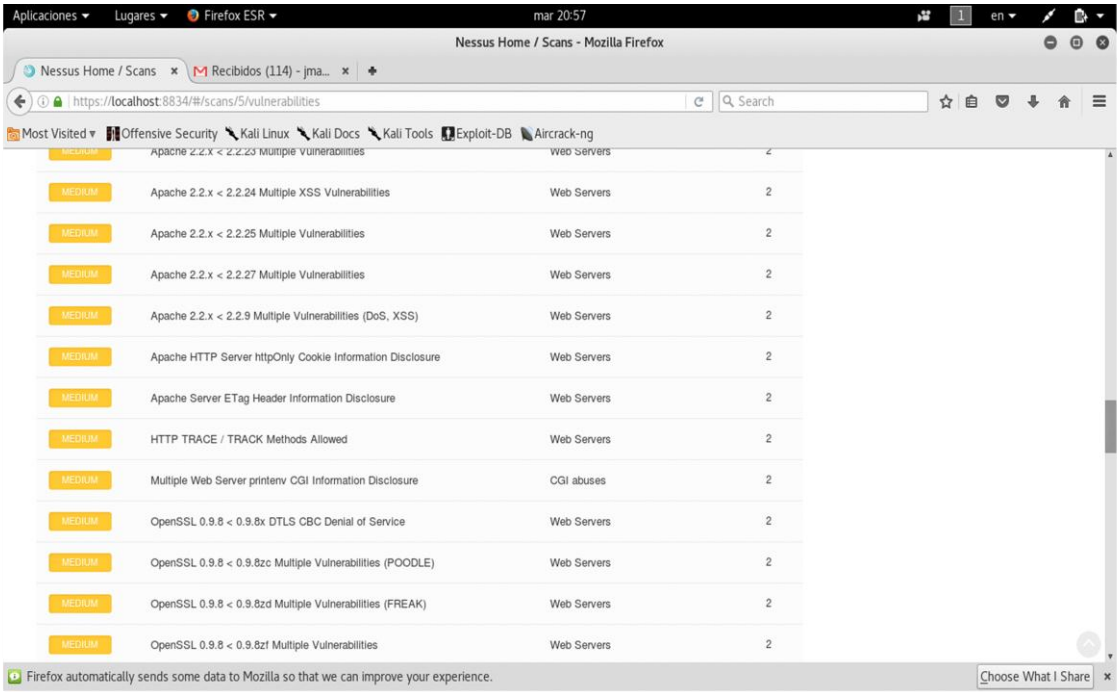


Figura # 21: Resultado de Scanner de Vulnerabilidades.

- Se encuentra que todos los usuarios son administradores del equipo.

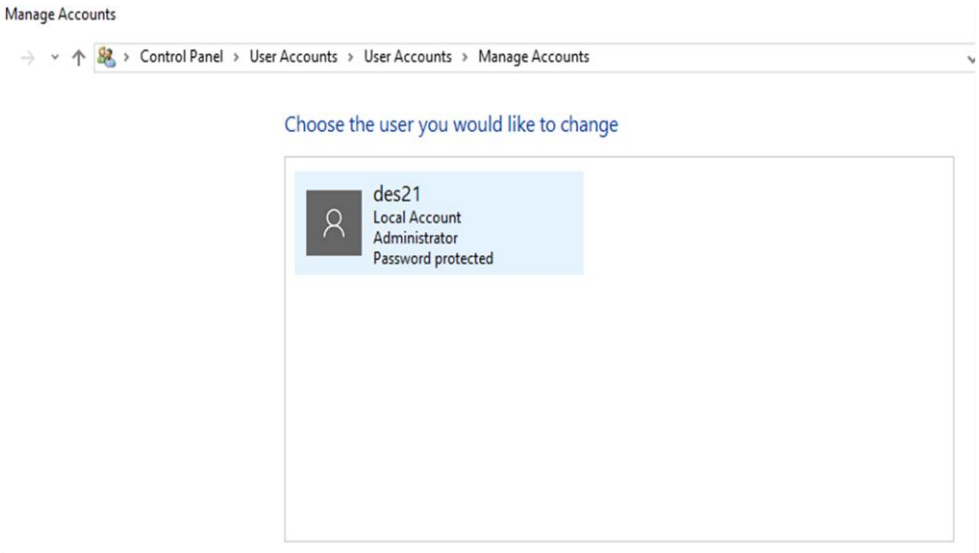


Figura # 22: ADMIN-USER.

- No existe control de filtrado de tráfico en la Red.

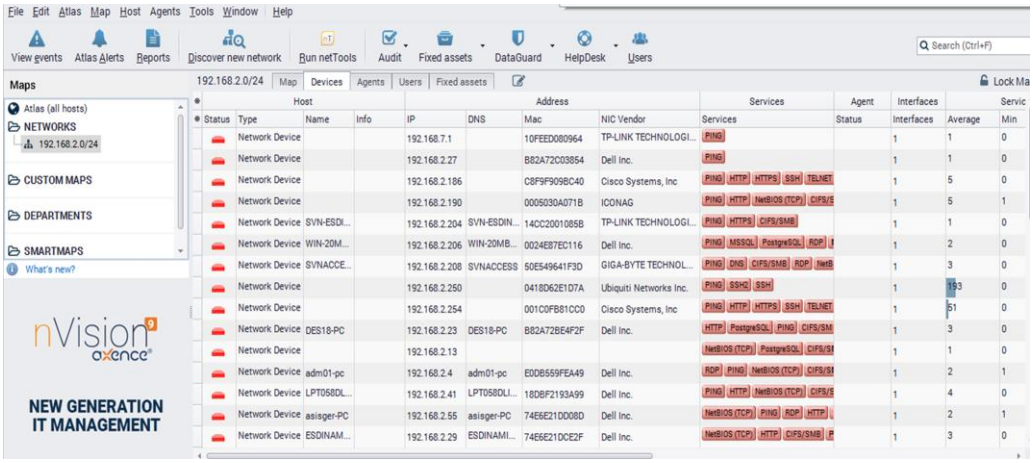


Figura # 23: Trafico de Red.

- Se encuentra ataques desde una red externa mediante el puerto 443.

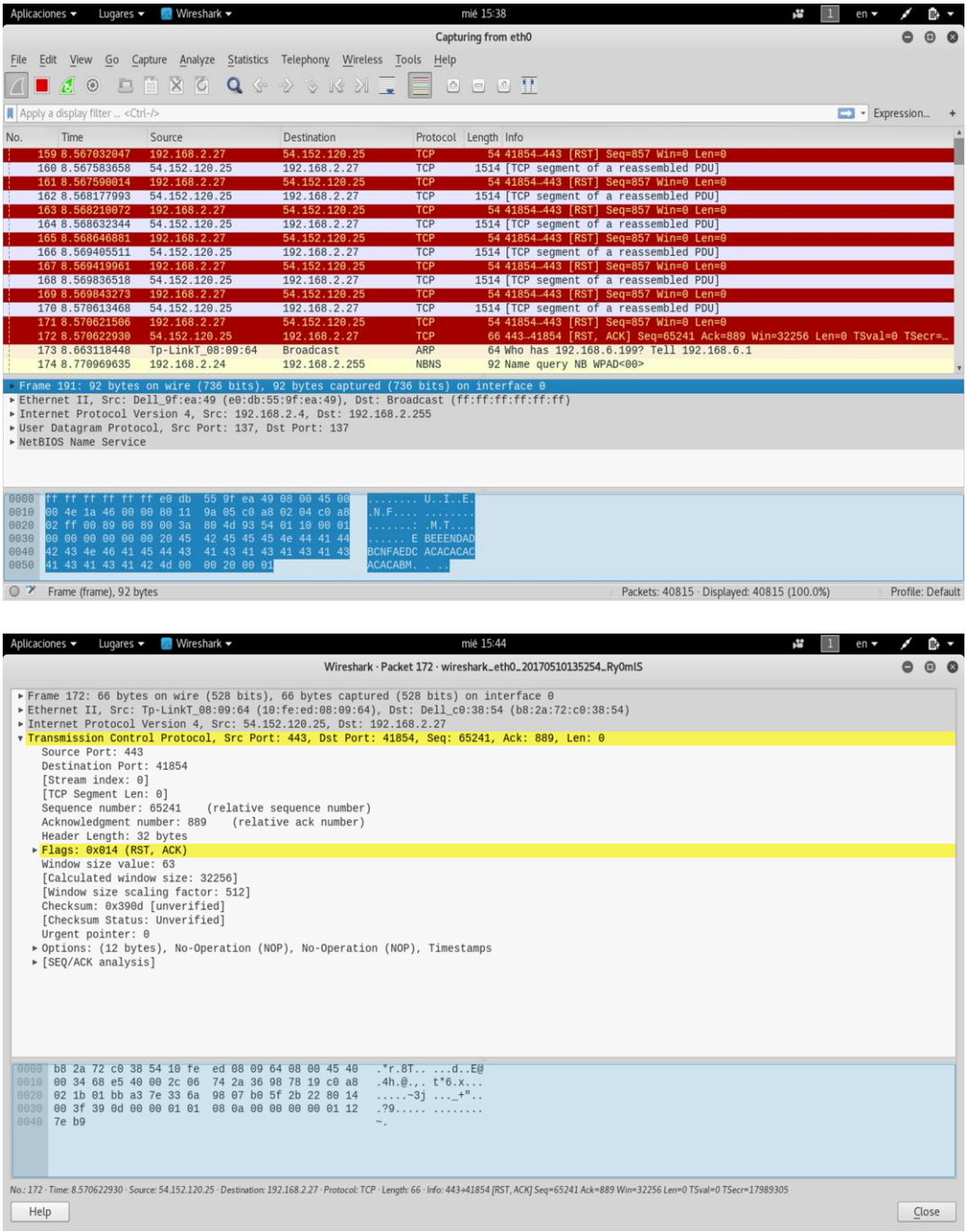


Figura # 24: Ataque a la red.

- Latencia de Red

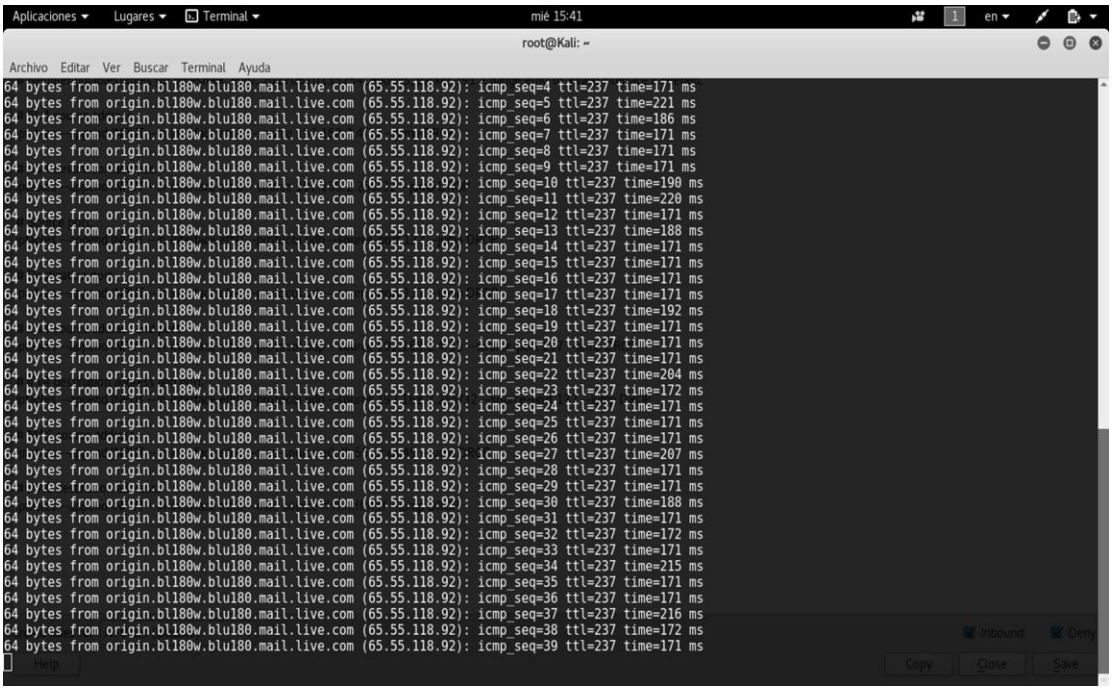


Figura # 25: Latencia de Red.

- Trazabilidad de la red hacia servidores de Hotmail.

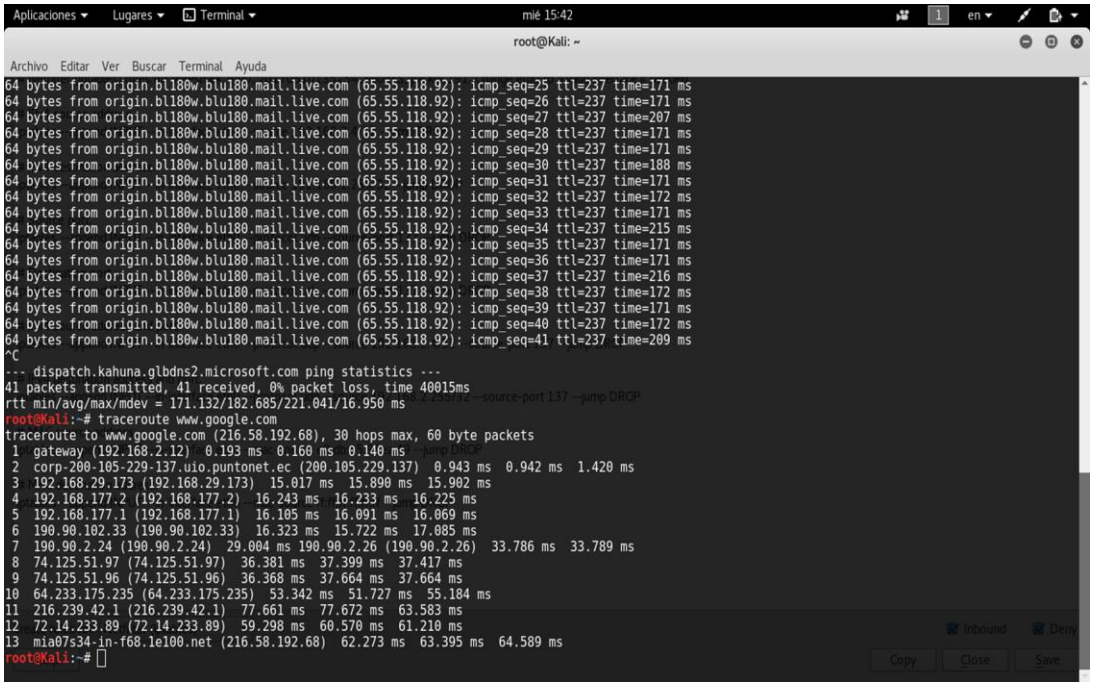


Figura # 26: Trazabilidad hacia servidores externos.

- Trazabilidad de la red.

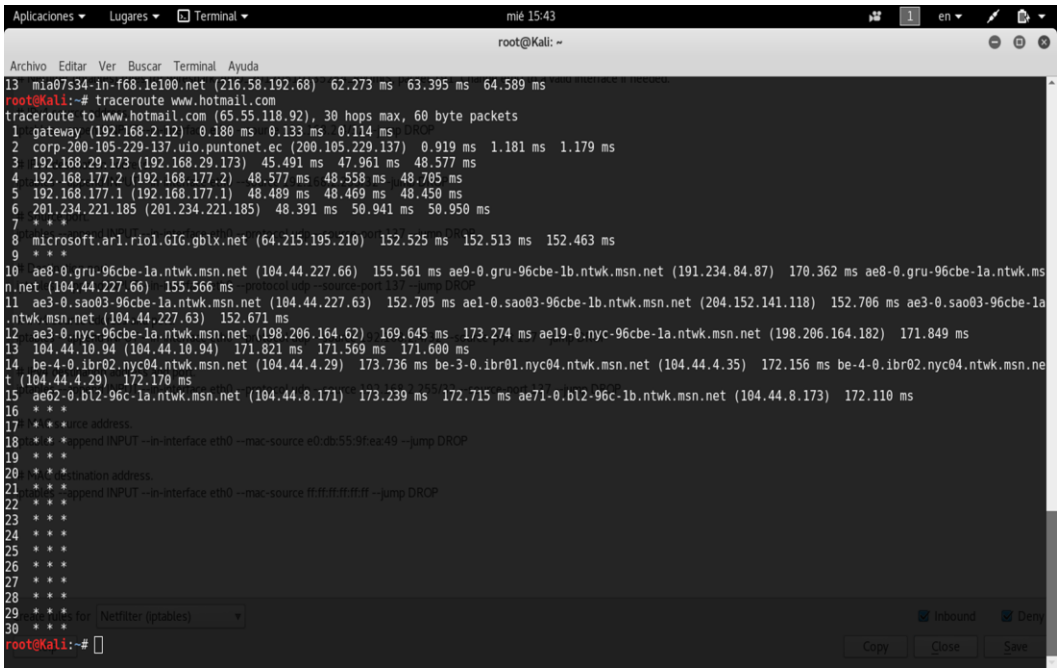


Figura # 27: Trazabilidad.

- Existen servidores y equipos de usuario final que no están actualizados con los suplementos de seguridad críticos que liberan los fabricantes.

3.5.2. Pruebas no técnicas.

Se realiza entrevistas a cinco usuarios encontrando debilidades:

- Los usuarios pueden descargar fácilmente la información mediante medios electrónicos como USB, Cd, etc.
- No existe restricción de acceso al área donde se encuentran los servidores.
- Los usuarios tienen conocimiento global de las claves de acceso a la red Wiffi.
- Los usuarios no tienen la suficiente conciencia de las políticas de seguridad de la información.
- Recursos humanos no tiene registros de los resultados de las capacitaciones al personal respecto de las políticas de seguridad de la información.
-

3.6. Detalles de los equipos de red existentes.

Tabla # 1: Equipos Informáticos.

TIPO de DISPOSITIVO	PREVIEW	MARCA /MODELO	CARACTERISTICAS
Switch 24 Puertos		D-link DGS-1024D	Switch de capa 2 de 24 puertos Ethernet sin consola. No tiene ninguna configuración.
Modem ADSL		DIR-600	Posee una antena omnidireccional de 5 dbi de ganancia compatible con 802.11b/g/n trabaja en la banda de 2,4 GHz, tiene 4 puertos FastEthernet LAN y 1 WAN, ofrece300 Mbps promedio, Tiene habilitado DHCP, soporta seguridad WEP y WPA2, administra un tráfico 8 PCs con tarjeta de red inalámbrica o Laptops.
Servidor de Aplicaciones		Del PowerEdge T20	Posee Intel Xeon E3, C226, 4 x UDIMM, Windows Server 2012 R2, 8 RAM, 16 Processors, 4TB HDD. Tiene habilitado sistema contable.
Servidor Web		Del PowerEdge T20	Posee Intel Xeon E3, C226, 4 x UDIMM, 8 RAM, 16 Processors, 4TB HDD, Windows Server 2012 R2. Utilizado como servidor Web.

Servidor de Exchange		Del PowerEdge T20	Posee Intel Xeon E3, C226, 4 x UDIMM, 8 RAM, 16 Processors, 4TB HDD, Windows Server 2012 R2 con Exchange 2010. Tiene habilitado la administración de cuentas de mail.
Router inalámbrico		Ubiquiti Unifi APC-AC PRO	Posee una antena omnidireccional de 5 dbi de ganancia compatible con 802.11b/g/n trabaja en la banda de 5X Faster con Dual-Radio 3x3 11AC, ofrece 450 Mbps promedio, Tiene habilitado DHCP, soporta seguridad WEP y WPA2, administrado mediante portal web, habilitado hasta 6 4 PCs con tarjeta de red inalámbrica o Laptops.
Equipo Portátil (Administrativo)		Lenovo Thinkpad E450	Procesador 5ta GEN, I5-52501 (3mcache 2.2 Gz) Sistema Operativo Windows 7. Pantalla de 14” HD 1366x768, Graphic Intel® 5500. RAM 4G – HDD 1TB
Pc de escritorio (Usuarios)		PC HP	PC408HPQ68 HP ProDesk 400 G3 SFF Ci5 6500 8GB, 1TB, DVDRW, W10 Pro
Impresora Matricial (Contabilidad)		EPSON fx-890	Matricial de impacto, 2 x 9 agujas, Bidireccional con búsqueda lógica, 1 original + 5 copias 1 original + 6 copias alimentación con tractor pull.

Impresora Multifunción (Usuarios)		Xerox WorkCentre 3655	Multifunción, Copia Correo Electrónico, Scanner Lector de tarjetas LRFID Integrado hasta 47 PPM, Fax Internet, Server Fax

Capítulo IV

4.1. Desarrollo del plan de contingencia bajo la norma ISO 27001:2013.

4.1.1. Necesidad de la implementación de un SGSI.

Una vez detallado las características esenciales de la norma ISO/IEC 27001:2013 así como presentar la situación actual de la empresa Booknowledge en lo referente a sus activos de información, topología de red y sus políticas de información, es preciso plantear como objetivo principal de este capítulo la implementación del SGSI basado en la norma ISO/IEC 27001:2013, para lo cual se describe a continuación los requerimientos para la seguridad de la información en la empresa así como también la forma de análisis de riesgos, simultáneamente con políticas de aceptación, procesos de control y eliminación de los riesgos y amenazas encontradas en el análisis de los activos de información de la empresa. (Villacis, 2016) (ISO 27001 , 2013)

Para lo cual se comprenderá como activos de la información a todo aquel dispositivo de software o hardware que administre o guarde información. Los activos de información de una empresa son muy importantes y valiosos hoy en día, para el caso de la empresa Booknowledge se ha enfocado en mitigar las amenazas a la seguridad de la información y ataques en su oficina matriz y en él se ejecutará el análisis de la implementación del SGSI, tomando en cuenta que existen servidores, dispositivos de conectividad y redes que permiten el correcto funcionamiento de la empresa entregando servicios a sus usuarios internos. (Villacis, 2016) (Hernandez Pinto, 2006)

Para todo esto se procederá con la aplicación del método de CUALIFICACIÓN O ESTIMACIÓN CUALITATIVA DEL RIESGO – BAJO – MEDIO – ALTO – GRAVE. (Villacis, 2016) (ISO 27001 , 2013)

4.1.2. Diseño del SGSI.

El mejor conjunto de procesos a ser tomado en cuenta para el desarrollo de un SGSI es el modelo PDCA, a continuación, se presenta un esquema de la utilización de estos procesos y cómo será el camino tomado para el desarrollo e implementación del sistema SGSI. Se deberá tener en cuenta la definición del alcance del SGSI, la política y objetivos, la identificación y evaluación de riesgos, la selección de los objetivos de control, el desarrollo del plan de tratamientos de riesgos y del enunciado de aplicabilidad para terminar con el desarrollo de las políticas de seguridad de la información en base a los controles de la norma ISO/IEC 27001:2013. (ISO 27001 , 2013)

En la siguiente figura se pretende dar a entender al usuario cuales son los pasos que seguir partiendo de modelos de referencia y recomendaciones propias de la norma para establecer un conjunto de procesos y reglas a ser tomadas en cuenta las cuales garantizarán un sistema seguro y estable.

4.2. Estableciendo el SGSI.

4.2.1. Alcance y límites del SGSI - Documento A.1.

Booknowledge busca especificar lineamientos que deben ser acatados por todo su personal de tal manera que pueda prever, corregir y actuar ante un evento que podría poner en riesgo la confidencialidad, integridad y disponibilidad de la información para sus usuarios internos y externos. (Villacis, 2016)

Hay que tener en cuenta que se establecen los límites y se propone un alcance al SGSI en base a las amenazas en la empresa debido a que este se ubica en su oficina matriz. (Villacis, 2016) (Hernandez Pinto, 2006)

4.2.2. Política y objetivos del SGSI - Documento A.2.

Como objetivo principal del SGSI se tiene que plantear las directrices a seguir por parte de los usuarios de la empresa, con el fin de salvaguardar la seguridad de la información, siendo el SGSI la base de conservación y evaluación de la seguridad dentro de la empresa.

Se deberá asignar un responsable de la Seguridad de la Información quien asegurará el mantenimiento permanente de los niveles de seguridad requeridos por la organización, lo que conlleva a entender que esta asignación tendrá el

compromiso de prevenir la ocurrencia de acciones inapropiadas o comportamientos ilegales de los distintos usuarios que puedan utilizar los recursos informáticos. (Villacis, 2016)

Estas responsabilidades tendrán que ir de la mano con las obligaciones legales, reguladoras y éticas que implican el buen funcionamiento y privacidad de la información de la compañía. El responsable o responsables de la seguridad también serán los encargados de documentar, actualizar e implantar las políticas contenidas en este documento como así mismo deberá realizar las evaluaciones periódicas para la valoración de la efectividad del SGSI y buscar posibles mejoras o modificaciones para la siguiente auditoría interna del sistema. (Villacis, 2016)

4.2.3. Valoración del riesgo – Documento A.3.

Se definirá un análisis de riesgos en función de los activos de la información de la compañía, presentando un análisis cualitativo y cuantitativo de los mismos basado en la arquitectura de procesos PDCA (Planear, Hacer, Chequear, Actuar), utilizando la Estimación Cualitativa del Riesgo - Método Triple Criterio – PGV (Probabilidad de ocurrencia, Gravedad del daño, y Vulnerabilidad). Este análisis conlleva a definir un espectro de amenazas que han sido divididas en tres grandes grupos que son las amenazas humanas, tecnológicas y naturales. (Villacis, 2016).

Los parámetros por tomar en cuenta para un sistema de seguridad de la información serán medir la capacidad de garantizar la confidencialidad, integridad y disponibilidad de la información. Esto se lo puede apreciar en las siguientes tablas:

Activos de Información criterio de Disponibilidad. (DISP.)

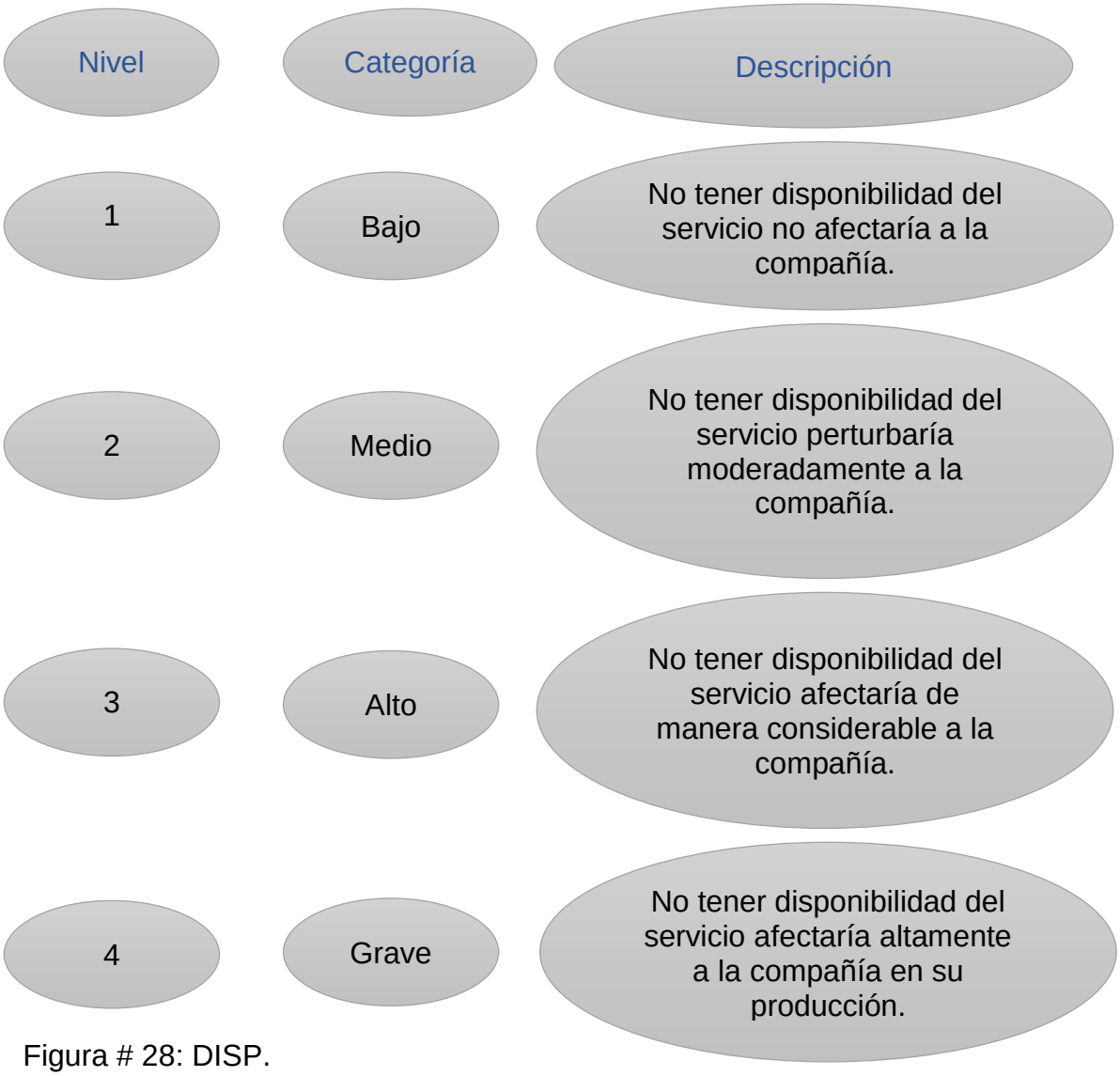


Figura # 28: DISP.

Activos de Información criterio de Integridad (INT.)

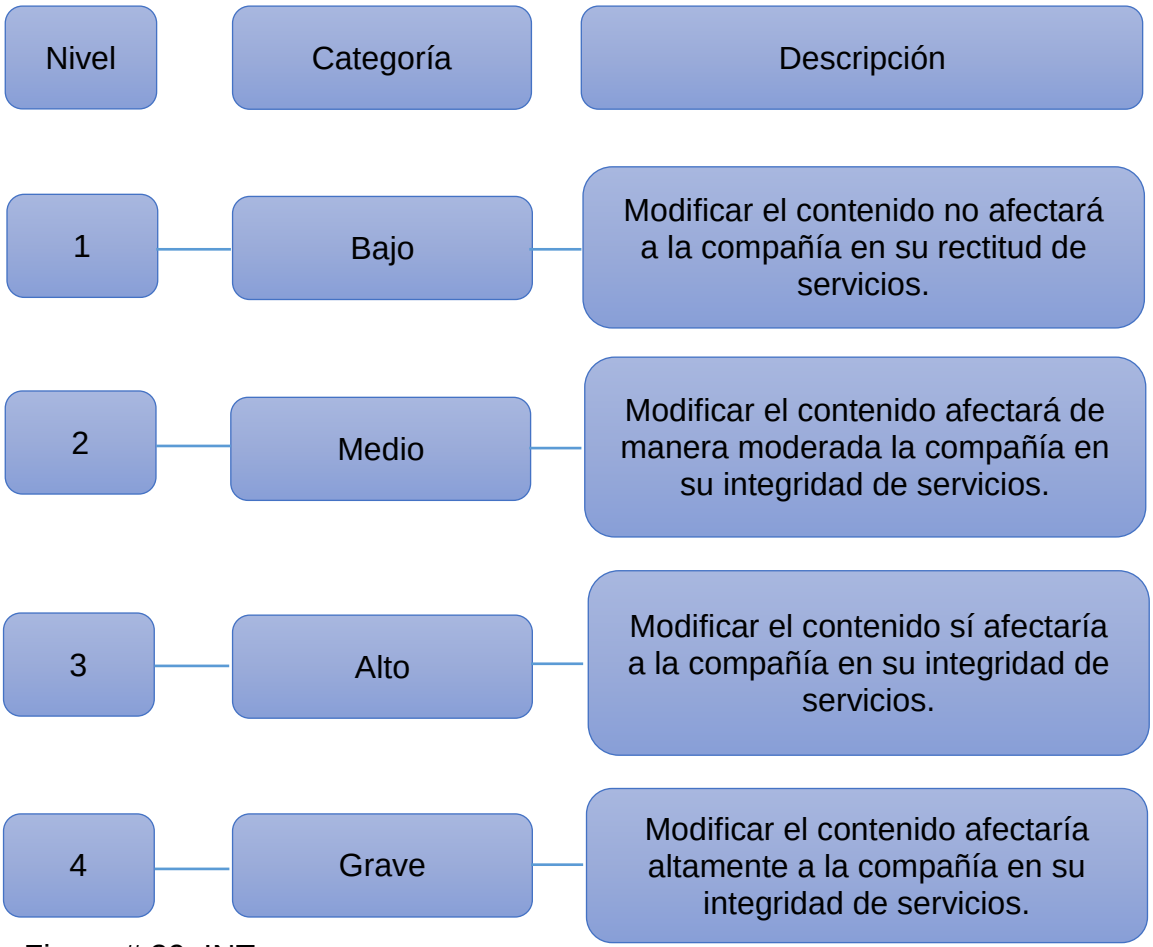


Figura # 29: INT.

Activos de Información criterio de Confidencialidad (CONF.)

Nivel	Categoría	Descripción
1	Bajo	Nivel muy bajo de riesgo su contenido puede ser descubierto sin causar mayor afectación a la compañía.
2	Medio	Su contenido puede ser revelado o compartido únicamente a personal de la compañía, no produciría mayor daño a la compañía.
3	Alto	Contenido de mayor importancia no se debería revelarlo más que al personal administrador del sistema de seguridad, nivel de afectación importante.
4	Grave	Contenido de mucha importancia que no debe ser revelado más que a las personas que presidencia autorice, el nivel de afectación de la compañía sería muy alto.

Figura # 30: CONF.

El nivel de importancia “NI” se lo define en la ecuación 1 y se lo detalla como el producto de estos tres factores (Confidencialidad, Integridad y Disponibilidad), que han sido detallados en las tablas anteriores lo que dará un valor entre 1 y 64 no mayor a este debido a que se tiene como valor más alto el producto de 4x4x4 que es igual a 64. (Villacis, 2016)

$$NI = CONF * INT * DISP$$

Ecuación 1 Nivel de importancia (Villacis, 2016).

Por consiguiente, una vez entendido cual será el valor mínimo y máximo del nivel de importancia y como se lo obtendrá a continuación en la tabla 6 se especifica los niveles de importancia fruto de aplicar la Ecuación 1. (ISO 27001 , 2013)

Rangos del Nivel de Importancia (NI)

Figura # 31: NI.

4.2.4. Amenazas, probabilidad de ocurrencia e impacto.

Otros parámetros a ser tomados en cuenta en el diseño del SGSI son los niveles de probabilidad de ocurrencia e impacto cuando se trabaja en la valoración de un riesgo, es por ello que en los cuadros siguientes se muestra este criterio.

Probabilidad de ocurrencia de un riesgo (PBBD.)

Nivel	Categoría	Descripción
1	Muy Improbable	La probabilidad de ocurrencia del riesgo es muy baja cerca del 1% al 25%.
2	Poco Improbable	La probabilidad de ocurrencia del riesgo se encuentra en el rango del 26% al 50%.
3	Improbable	La probabilidad de ocurrencia del riesgo se encuentra en el rango del 51% al 74%.
4	Probable	La probabilidad de ocurrencia del riesgo se encuentra en el rango del 75% al 95%.
5	Muy probable	La probabilidad de ocurrencia del riesgo se encuentra en el rango del 96% al 100%.

Figura # 32: PBBD.

Niveles de Impacto de un riesgo (IMPAC.)

Nivel	Categoría	Descripción
1	Imperceptible	Nivel de impacto muy pequeño o nulo un usuario afectado de la compañía.
2	Leve	Nivel de impacto pequeño poco tiempo de respuesta afectación de entre 2 a 10 usuarios de la compañía.
3	Medio	Nivel de impacto importante requiere mayor tiempo de respuesta de entre 11 y 50 usuarios de la compañía.
4	Alto	Nivel de impacto muy significativo requiere de mucho tiempo de respuesta, se afectan hasta 100 usuarios
5	Grave	Nivel de impacto catastrófico donde la mayoría de los usuarios de la compañía se verían aquejados, máximo tiempo de respuesta.

Figura # 33: IMPAC.

Para fines pertinentes del caso se debe comprender que los usuarios son los trabajadores de la compañía que en el momento de encontrarse con un nivel de impacto medio a grave se verían afectados en su rendimiento diario ya que los procesos de eliminación de riesgos o amenazas serán mayores, es decir implicaran mayor tiempo de respuesta, mayor costo a la compañía y con el riesgo de que se interrumpa las actividades por un daño mucho mayor.

A continuación, se procede a encontrar la ecuación del nivel de riesgo “NR”, tomando en cuenta que es otro parámetro por analizar para el desarrollo y diseño del SGSI ya que lo que se buscará a la final será tratar a cada uno de los riesgos encontrados y referenciarse a lo que la norma dice para el tratamiento de los riesgos.

La ecuación 2 permite calcular el Nivel de Riesgo en función de la probabilidad de ocurrencia e impacto.

$$NR = PBBD * IMPAC$$

Ecuación 2 Nivel de Riesgo. (Villacis, 2016).

El remplazo de los valores en la Ecuación 2 entrega la tabla 2 que muestra el nivel de riesgo adecuado.

Tabla # 2: Niveles de Riesgo.

Pbbd		Impacto		Nivel de Riesgo
1	Muy improbable	1	Imperceptible	Bajo
2	Poco improbable	1	Imperceptible	Bajo
3	Improbable	1	Imperceptible	Bajo
4	Probable	1	Imperceptible	Medio
5	Muy probable	1	Imperceptible	Alto
1	Muy probable	2	Leve	Bajo
2	Poco improbable	2	Leve	Bajo
3	Improbable	2	Leve	Medio
4	Probable	2	Leve	Alto
5	Muy probable	2	Leve	Alto
1	Muy improbable	3	Medio	Medio
2	Poco improbable	3	Medio	Medio
3	Improbable	3	Medio	Alto
4	Probable	3	Medio	Alto
5	Muy probable	3	Medio	Grave
1	Muy improbable	4	Alto	Alto
2	Poco improbable	4	Alto	Alto
3	Improbable	4	Alto	Grave
4	Probable	4	Alto	Grave
5	Muy probable	4	Alto	Grave
1	Muy improbable	5	Grave	Alto
2	Poco improbable	5	Grave	Grave
3	Improbable	5	Grave	Grave
4	Probable	5	Grave	Grave
5	Muy probable	5	Grave	Grave

Con esta tabla se pretende indicar cuáles serían los niveles de riesgo, el impacto y la probabilidad de que un evento adverso de darse podría alterar el correcto funcionamiento de la compañía en su día a día. A su vez estos parámetros serán tomados en cuenta para el tratamiento de los riesgos como la norma ISO/IEC 27001:2013 lo recomienda.

4.2.5. Análisis de costos de las amenazas.

Como se puede notar hasta el momento el análisis presentado solo se ha enfocado al tratamiento de los riesgos y a la afección que estos pudieran presentar en la confidencialidad, integridad y disponibilidad de la información para los usuarios internos de la compañía, mas no así en un factor que realmente es muy importante para la economía de la compañía como es el análisis en los costos de estas amenazas o riesgos que puedan presentarse ya que evidentemente es un valor que por lo general no es tomado en cuenta en el presupuesto anual o si es tomado en cuenta se lo prevé con un valor pequeño dentro de los rubros de mantenimiento de la infraestructura como tal.

En la tabla 2 se muestra un análisis de los costos que será un factor nuevo de cálculo para ser tomado en cuenta en siguientes procesos para el diseño del SGSI.

Costos de las Amenazas
(COS)

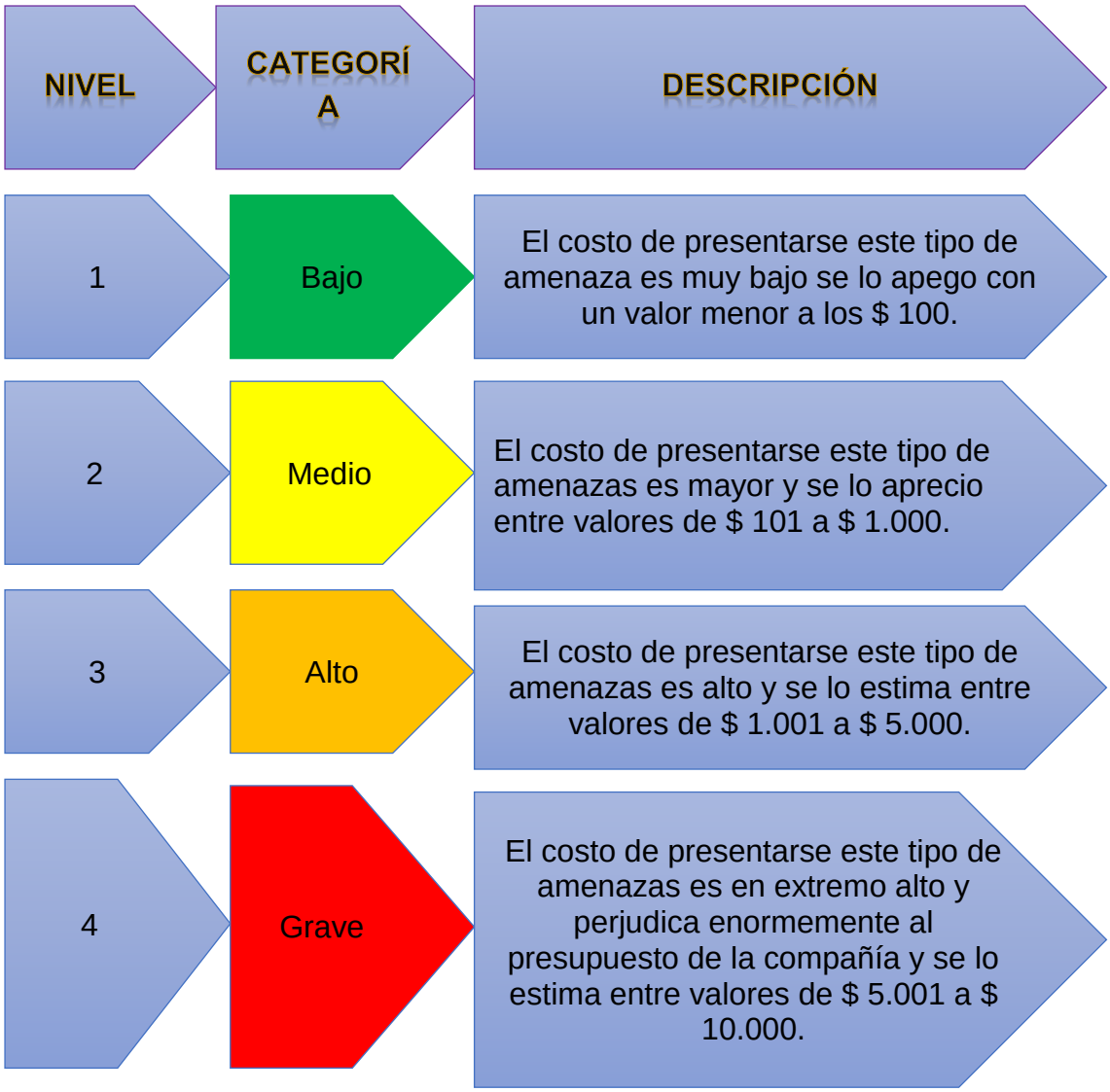


Figura # 34: COS.

Como se puede ver se tiene 4 niveles de costos donde sus rubros de perdidas van variando de acuerdo con cada nivel, se debe tomar en cuenta los niveles 3 y 4 donde realmente los costos ya representan egresos muy altos a la compañía, y es en estos niveles en donde se debe evitar caer, es así como la norma ISO justamente prevé que estos daños se den o su probabilidad de ocurrencia sea mínima. De todas maneras, hay que pensar como se lo demuestra en la tabla 2 que si hay una probabilidad de que esto ocurra y la compañía debe estar preparada y lista con su plan de contingencia para el evento.

4.2.6. Cálculo del riesgo.

Una vez definidas todas las variables con sus niveles en cada una de las tablas anteriores se procede a relacionarlas entre sí para por medio de la ecuación 3 expresar el valor del cálculo del riesgo.

$$RIESGO = PBBD * IMPAC * COS$$

Ecuación 3. Cálculo del Riesgo. (Villacis, 2016)

Al fijarse en la Ecuación 3 se puede apreciar que si asociamos dos de los factores como son la probabilidad y el impacto (PBBD * IMP) y comparando con la ecuación 2 se puede reemplazar la ecuación 2 en la Ecuación 3 obteniendo la Ecuación 4 que define el cálculo del riesgo de la siguiente manera, donde:

NR = Nivel de Riesgo

COS = Costo de Amenazas

$$RIESGO = NR * COS$$

Ecuación 4. Cálculo del Riesgo en función del Nivel de riesgo. (Villacis, 2016).

Corresponde ahora comprender que el Riesgo quedará definido entre un rango de 1 a 100 debido a que se tienen 5 niveles de probabilidad y de impacto respectivamente y 4 niveles de costos como lo indican la tabla 2, al ser un rango entre 1 y 100 se procederá a definir 4 niveles o rangos de riesgos que serán tomados en cuenta en la gestión del SGSI para el tratamiento de las amenazas y de los riesgos, así como definir que controles utilizar para mitigar los valores altos y la política de aceptación de los de menor valor.

En el cuadro 3 se indica los rangos de riesgo a ser tomados en cuenta en la implementación del SGSI.

Rango de Riesgos.

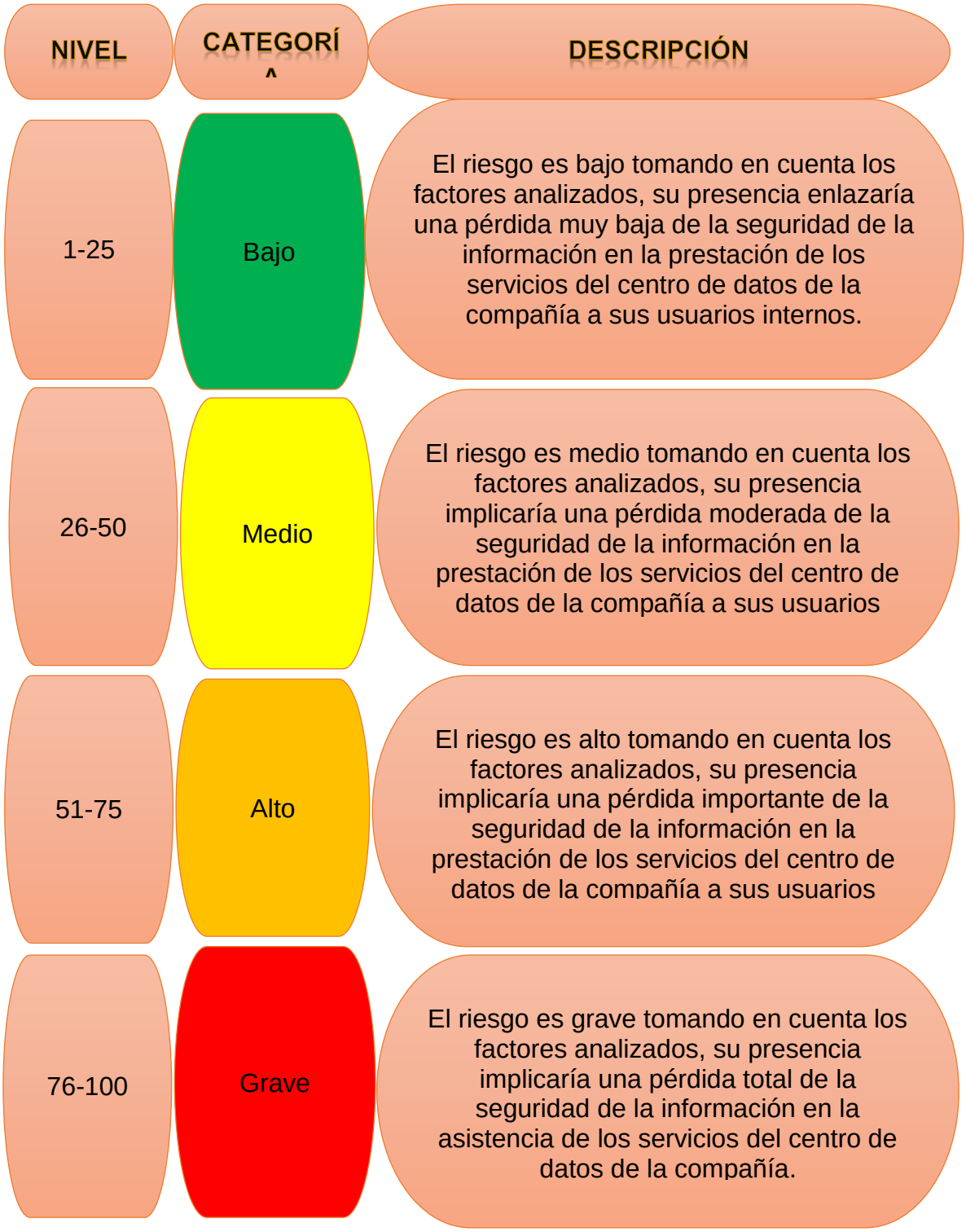


Figura # 35: Rango de riesgos.

4.2.7. Necesidad de la implementación de un SGSI.

Cabe mencionar que todo este análisis del tratamiento del riesgo se basa en las recomendaciones que la norma ISO/IEC 27001:2013 presenta, definiéndolas como:

- Aplicar Controles.
- Aceptar el Riesgo.
- Evitar el Riesgo.
- Transferir el Riesgo.

En vista de estas cuatro recomendaciones que la norma propone se consideran tres de ellas como dependientes de los valores de probabilidad e impacto las cuales son: las tres primeras de la lista anterior y recomienda transferir el riesgo en caso de que el activo de información dependa de un agente externo al centro de datos de la compañía.

En el cuadro 10 se muestra este criterio en base a la recomendación de la norma y en base al nivel de riesgo definido.

Tratamiento del Riesgo.

Nivel de Riesgo	Acción a Tomar
Bajo	Aceptar el Riesgo
Medio	
Alto	Aplicar Controles
Grave	

Figura #36: Tratamiento de riesgos.

4.2.8. Análisis y evaluación del riesgo adjudicación de controles - Documento A.4.

Para hacer el análisis y evaluación de los riesgos se debe identificar las amenazas o definirlas con criterio por parte del desarrollador del SGSI a las que los activos de información están sometidos, de esta manera se las evalúa tomando en cuenta lo que indica el Documento A.3 estimando las probabilidades de ocurrencia, impactos comerciales y costos, dando origen a la matriz de riesgos del centro de datos de la compañía, esta matriz es la que permitirá aplicar los controles y recomendaciones que la norma ISO/IEC 27001:2013 recomienda garantizando así la seguridad de la información y la continuidad de la misma.

Es necesario indicar que a más de utilizar las relaciones y variables del Documento A.3 los tipos de amenazas que han sido analizadas pertenecen a tres grandes grupos que son:

- Humanas.
- Técnicas.
- Naturales o Ambientales.

Estos tipos de amenazas abarcan todo el espectro de daños que pudieran sufrir los activos de la información de la compañía.

A continuación en las tablas 2, 3,4, 5, se muestra la identificación de los riesgos encontrados en la compañía de acuerdo al espectro de amenazas definido, para esto se ha tomado en cuenta la probabilidad de ocurrencia y el impacto que generaría esa amenaza, para ello se hace referencia a las tablas 5 y g donde se toman los valores a considerar para ser reemplazados en la ecuación 2 que indica el valor del nivel de riesgo NR, este valor se lo confronta con la tabla 2 quien será la que adjudique un color a ese parámetro, seguidamente de ello se hace referencia a la tabla 3 que indica el costo de las amenazas para reemplazando esos valores en la ecuación 4 obtener el Riesgo total que de igual manera haciendo referencia se adjudicará un color de acuerdo a ese remplazo, finalmente el valor obtenido en el Nivel de Riesgo indicará que acción tomar con respecto a la amenaza.

Tabla # 3: Amenazas Humanas

IDENTIFICACIÓN DE LOS RIESGOS EN F(A.3)			CÁLCULO Y EVALUACIÓN DEL RIESGO PARA EL CENTRO DE DATOS DE BOOKNOWLEDGE.					
AMENAZAS	**VULNERABILIDADES**	**IMPACTO**	**PBBD**	**IMPAC**	**NR**	**COS**	**RIESGO**	**ACCION A TOMAR**
Desconfiguración involuntaria de equipos con nivel de importancia GRAVE.	Gestión inadecuada de claves de configuración, al igual que no existe una politica de acces o a las configuraciones, así como también no hay un proceso de almacenamiento de las mis mas.	La desconfiguración de un equipo de red como un switch o un enrutador u otro dispositivo de red incidirá mucho en el des empeño del centro de datos y de la empresa en sí, ya que se puede tener problemas de direccionamiento y enrutamiento externo.	3	5	15	3	45	Aplicar Controles
Desconfiguración involuntaria de equipos con nivel de importancia ALTO.			3	4	12	2	24	Aceptar el Riesgo
Desconfiguración involuntaria de equipos con nivel de importancia MEDIO.			4	3	12	2	24	Aceptar el Riesgo
Desconexión de puertos en los equipos de red con nivel de importancia GRAVE.	No existe control de ingres o al Centro de datos, al igual que no existe protección física adecuada para evitar la desconexión de puertos, no hay una politica de reemplazo o cambio de cableado de los puertos si fuese necesario.	La desconexión de puertos en un equipo de red o de un activo de la información podria dejar sin servicio a varios usuarios de la empresa o incluso a todos los usuarios de la misma.	3	5	15	3	45	Aplicar Controles
Desconexión de puertos en los equipos de red con nivel de			3	4	12	2	24	Aceptar el Riesgo
Desconexión de puertos en los equipos de red con nivel de mportancia MEDIO.			4	3	12	2	24	Aceptar el Riesgo
Ingreso a la configuración de equipos con nivel de importancia GRAVE.	No hay un bloqueo de acceso a los equipos por agentes externos, no hay una politica de monitoreo y de regi tro de ingres o a las configuraciones de los equipos, no existe una politica formal de concesión de claves de acceso.	El cambio de configuración sin autorización de un equipo de red o de un activo de la información afectará el desempeño diario de la empresa.	3	5	15	3	45	Aplicar Controles
Ingreso a la configuración de equipos con nivel de importancia ALTO.			3	4	12	2	24	Aceptar el Riesgo
Ingreso a la configuración de equipos con nivel de importancia MEDIO.			4	3	12	1	2	Aceptar el Riesgo

Adaptado de (Villacis, 2016).

Tabla # 4: Identificacion de Amenazas Humanas

IDENTIFICACIÓN DE LOS RIESGOS EN F(A.3)			CÁLCULO Y EVALUACIÓN DEL RIESGO PARA EL CENTRO DE DATOS DE BOOKNOWLEDGE.					
AMENAZAS	VULNERABILIDADES	IMPACTO	PBBD	IMPAC	NR	COS	RIESGO	ACCION A TOMAR
Suplantación de Identidad.	No existe una politica de gestión de claves de usuario y no hay un monitoreo de las mismas.	Violación de la confidencialidad e integridad de los activos de la información, peligro de robo y ataques .	4	4	16	2	32	Aplicar Controles
Alteración de la información contenida en los equipos.	No exis te una politica de autorización de cambios migraciones o actualizaciones.	Cambios no autorizados genera conflictos entre usuarios por desconocimiento de cambios.	4	3	12	3	36	Aplicar Controles
Mal manejo de Equipos.	No existe una politica de uso decuado de los equipos, ni sanciones por afectación a los mismos.	Mal manejo de los activos de la información podria ocasionar daño parcial o total del equipo afectando información sensible.	4	3	12	3	36	Aplicar Controles
Daño de equipos por mal mantenimiento.	No se tiene una politica de mantenimiento preventivo y correctivo de los equipos.	Mal mantenimiento preventivo y correctivo de equipos afectaria el desempeño diario de la compañia.	2	5	10	4	40	Aplicar Controles
Robo o perdida de Equipos.	No existe un inventario completo de los activos de información, no se establece de manera formal los propietarios de los equipos.	Perdida económica, perdida de tiempo, interrupción de labores momentánea del us uario interno de la compañia.	2	5	10	4	40	Aplicar Controles

Adaptado de (Villacis, 2016).

Tabla # 5: Amenazas Tecnologicas.

IDENTIFICACIÓN DE LOS RIESGOS EN F(A.3)			CÁLCULO Y EVALUACIÓN DEL RIESGO PARA EL CENTRO DE DATOS DE BOOKNOWLEDGE.					
AMENAZAS	VULNERABILIDADES	IMPACTO	PBBD	IMPAC	NR	COS	RIESGO	ACCION A TOMAR
Fallas en el s ervicio del proveedor (ISP).	No existe un proveedor de Backup en el caso de que falle el principal de la empresa.	En la actualidad prescindir de servicios de internet es un gran problema para la empresa.	3	5	15	3	45	Aplicar Controles
Falla en el funcionamiento de un equipo con nivel de importancia GRAVE.	No hay un procedimiento formal de contingencia, al igual que no existe un procedimiento formal de almacenamiento de configuraciones; imposibilitando el funcionamiento normal de la empresa de darse es te tipo de amenaza.	Afectaria gravemente el desempeño diario de la empresa afectando altamente en sus finanzas.	3	4	12	3	36	Aplicar Controles
Falla en el funcionamiento de un equipo con nivel de importancia ALTO.		Afectaria considerablemente el desempeño diario de la empresa afectando considerablemente en sus finanzas.	3	4	12	2	24	Aceptar el Riesgo
Falla en el funcionamiento de un equipo con nivel de importancia MEDIO.		Afectaria de manera moderada el desempeño diario de la empresa afectando moderadamente en sus finanzas.	3	3	9	2	18	Aceptar el Riesgo

Adaptado de (Villacis, 2016).

Tabla # 6: Amenazas Tecnologicas

IDENTIFICACIÓN DE LOS RIESGOS EN F(A.3)			CÁLCULO Y EVALUACIÓN DEL RIESGO PARA EL CENTRO DE DATOS DE BOOKNOWLEDGE.					
AMENAZAS	VULNERABILIDADES	IMPACTO	PBBD	IMPAC	NR	COS	RIESGO	ACCION A TOMAR
Daño en medios de transmisión	No se cumplen normas de cableado estructurado.	Afectación directa a un usuario o grupo de usuarios de la compañia.	3	3	9	2	18	Aceptar el Riesgo
Interferencia entre cables eléctricos y de comunicaciones.	No se cumplen normas de cableado estructurado.	Afectación directa a un usuario o grupo de usuarios de la compañia por presencia de perdidas en la trasmisión.	2	2	4	1	4	Aceptar el Riesgo
Virus , troyanos , gusanos , ataques específicos.	No hay un sistema de detección y monitoreo de amenazas o ataques, falta de seguridades, y no se instruye al personal sobre estas amenazas.	Afectación en la confidencialidad e integridad de los servicios a los usuarios de la compañia, incluso daño parcial o total del equipo.	4	4	16	3	48	Aplicar Controles
Incapacidad de proveer s ervicio a los us uarios internos de la compañia	No existe plan de contingencia ni un centro de datos de backup.	Impide correcto desempeño de los usuarios internos de la compañia incluye perdidas económicas.	2	3	6	2	12	Aceptar el Riesgo
Falla en los grupos de respaldo.	No se tiene politica de mantenimiento preventivo y periódico de estos equipos.	En caso de cortes de alimentación eléctrica no cumplirian con su cometido de dar respaldo.	2	3	6	3	18	Aceptar el Riesgo
Falla en el sistema de climatización del centro de datos.	No se tiene politica de mantenimiento preventivo y periódico de estos equipos.	Graves daños en el centro de datos de la compañia con una afectación económica considerable.	2	3	6	3	18	Aceptar el Riesgo

Adaptado de (Villacis, 2016).

Como se puede apreciar en las figuras antes mencionadas se presenta el cálculo del riesgo en función del documento A.3, y se determina la metodología del tratamiento de cada riesgo que se la ha definido como la acción a tomar, como se indicó anteriormente se van aplicar controles a partir de niveles de riesgo medio, alto, y grave, a pesar de que en ninguno de los casos el nivel de riesgo llega a ser GRAVE si llega a los límites del nivel de riesgo ALTO.

4.2.9 Selección de objetivos de control y controles - Documento A.5.

Para la selección de objetivos de control y los controles a ser aplicados se lo hará en función de la norma ISO 27001:2013 sugiere, para esto en base a las amenazas descritas se analizará cada uno de los casos en donde la acción a tomar sea “Aplicar Controles” y se escogerá el más adecuado proveniente de la norma ISO. Para fines de este proyecto de titulación se hará también un análisis de los objetivos de control y controles a ser tomados en cuenta cuando la acción a tomar sea “Aceptar el Riesgo”. (Villacis, 2016).

Hay que tomar en cuenta que para el conjunto de amenazas definidas existen varios objetivos de control y controles que la norma entrega en su anexo A, por lo que es necesario saber escoger el objetivo de control y controles necesarios para mitigar esta amenaza sin que esto signifique escoger todos.

De igual manera también se indicará que existen objetivos de control y controles considerados como fundamentales o básicos para la existencia de un SGSI, y serán aquellos que podrán ser aplicables para el tratamiento de todas las amenazas identificadas divididas en sus tres grandes grupos ya conocidos anteriormente.

Las tablas 4 y 5 del se indica los objetivos de control y controles seleccionados, considerados como fundamentales o básicos para las amenazas del tipo HUMANAS es decir estos objetivos de control y controles serán implementados siempre a más de los que hayan sido escogidos como específicos para cada amenaza en particular.

En las tablas 3 a 6 se encuentran los controles individuales para cada una de las amenazas humanas.

De inmediato en las tablas 4 y 5 se muestran los controles y objetivos de control considerados comunes para las amenazas tecnológicas, seguidamente de ello en la tabla 6 se muestran los objetivos de control y controles individuales para las amenazas tecnológicas con acción a tomar “Aplicar Controles”.

En las tablas 4 a 6 se muestran los objetivos de control y controles seleccionados para las amenazas tecnológicas con la acción a tomar “Aceptar el Riesgo”.

Finalmente, en las tablas 5 y 6 se muestran los objetivos de control y controles para las amenazas naturales con el particular que son para los dos tipos de acciones a tomar como son “Aplicar Controles y Aceptar el Riesgo”.

Una vez seleccionados los objetivos de control y controles para cada una de las amenazas seleccionadas y a ser tomadas en cuenta se procede a realizar un documento de aplicabilidad es decir se justificará por qué se han escogido ciertos objetivos de control.

4.2.10. Enunciado de aplicabilidad - Documento A.6.

Se procede a mostrar este enunciado de aplicabilidad del SGSI de la empresa Booknowledge, desarrollado en este proyecto de titulación indicando la justificación, como hacerlo y aplicabilidad de cada uno de los objetivos de control y controles escogidos, así como también de los controles no escogidos.

4.2.11. Procesos propuestos después de la selección de objetivos de control y controles - Documento A.7.

Se muestra los procesos que se recomienda poner en práctica para el correcto funcionamiento del SGSI a implementarse, estos procesos se basan en la norma ISO 27002 garantizando la disponibilidad, confidencialidad, e integridad de la información para efectos de tener un mejor entendimiento se los ha codificado en función de su nombre y un orden correspondiente.

Como se puede apreciar los procesos definidos han sido en base a los objetivos de control y controles escogidos previamente. Es de suma significación definir y dar a conocer al personal, para su correcta aplicación.

Como un ejemplo de proceso en la tabla 40 del anexo 3 se procederá a enunciar el proceso de política de seguridad de la información para el usuario interno de la compañía tomando en cuenta que será una política restrictiva.

Capítulo V

5.1 Conclusiones y recomendación.

5.1.1 Orientadas a las Empresas.

Las herramientas de tecnología se desarrollan con el pasar del tiempo volviéndose inseguras en la medida que su utilización no sea la más conveniente en la organización, convirtiéndose así en objeto de amenazas.

Hoy en día en toda compañía es una necesidad frecuente utilizar esquemas de seguridad fuertes, que admitan una mayor confiabilidad de la información utilizada para la toma de decisiones y en el trabajo propio de la empresa.

La incomprensión de la Gerencia que conlleva a la falta de apoyo económico a la gestión de la información para establecer medidas de seguridad estimula que la entidad tenga una exhibición mayor a los riesgos.

La seguridad de la información es un compromiso compartido de todos los niveles de la organización, que solicita del apoyo de todos ellos, pero debe estar regida por un plan y con la adecuada coordinación.

5.1.2 Orientadas al Tema de Tesis.

El adelanto de la tecnología y del conocimiento de los seres humanos ya sean usadas con buena o mala intención, vuelven más vulnerable a la información, por lo tanto, se presentan diversas amenazas tanto internas como externas volviéndola poco confiable.

La evaluación de seguridad informática ejecutada a la empresa Booknowledge dio a conocer a todo el recurso humano que en ella laboran, los riesgos a los que está expuesta la información y que directa o indirectamente ellos favorecen para que estos aumenten.

La elaboración de este trabajo de tesis, ayudo a que la compañía Booknowledge tome conciencia de cuán importante es que la información sea confiable, integra y disponible para la organización ya que pueden observar que si cualquiera de estas características sufriera alteraciones conllevaría a resultados nefastos para la entidad.

En la ejecución del SGSI de la compañía se debe seguir un proceso para lo cual se identificó a los activos de información, pronto se conoció políticas de seguridad implementadas en la entidad, posteriormente se recopiló amenazas

o ataques detectados; este proceso permitió (Hernandez Pinto, 2006) conocer y tabular los niveles de riesgo, niveles de importancia, probabilidad de ocurrencia, impacto, etc. Finalmente, se eligió los objetivos de control y controles que mitiguen estas amenazas y ataques bajo la norma tratada.

Los controles elegidos dentro de los objetivos de control resultan de gran provecho para el tratamiento de los riesgos descubiertos en el centro de datos de la compañía, su correcta implementación mitigaría las amenazas en su gran mayoría.

5.2. Recomendaciones.

5.2.1. Orientadas a las Empresas

- Precisar políticas de seguridad claras. No solo por los riesgos originados en los equipos de informática o de los servicios que ofrece el área de sistemas, sino también por las pérdidas de productividad que puede crear un suceso de seguridad
- Se recomienda crear en las organizaciones la administración de seguridad de la información, es decir implicar a todos los jefes de áreas en la administración de la seguridad con el apoyo total del Departamento de Sistemas.
- Fomentar la conciencia del empleado para avalar que no haya fuga de información.
- Elaborar Auditorías a la seguridad de la información de sus compañías para tener un juicio de sus vulnerabilidades y las medidas a seguir para minimizar los riesgos.
- Suministrar al área de sistemas en lo posible los recursos necesarios para mantener la seguridad informática en la compañía.

5.2.1. Orientadas al Tema de Tesis.

- En el Departamento de sistemas se debe contar con personal cuya ocupación sean las de administrar la seguridad de la información en la compañía.
- Se debe reubicar el Departamento de Sistemas tomando en cuenta que el área no esté próxima a corredores de alto tráfico de personas.
- La empresa Booknowledge deberá ejecutar un análisis de riesgo cada cierto tiempo. Este periodo de tiempo deberá establecerse según el impacto de riesgo en el que se halle la organización.
- El personal representante de la seguridad de la información deberá monitorear constantemente los elementos de riesgos existentes en la organización.
- Se recomienda organizar políticas de seguridad en base a los resultados del análisis de riesgo. Estas políticas serán claras para el correcto entendimiento por parte de todo el personal.
- Establecer las políticas de seguridad recomendadas en este trabajo.
- Trazar un plan estratégico de seguridad con la guía que este trabajo propone.
- La Gerencia de la empresa Booknowledge, deberá sancionar al personal que infrinja la política de seguridad de acuerdo con el reglamento establecido para estos casos.
- Renovar el Plan de Seguridad de Información con cada valoración de riesgo de la empresa.
- El personal que está involucrado en el plan estratégico de seguridad debe estar realmente comprometido con la realización de mismo.
- La gerencia debe ofrecer soporte completo para la implementación de este plan estratégico de seguridad informática.

Referencias

Flores , E., & Jiménez Nuñez. (2010).

Hernandez Pinto, M. (2006). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial.

ISO 27001 , S. (18 de marzo de 2013). *ISO 27001 Security*. Obtenido de http://www.iso27001security.com/html/27000.html

ISO/IEC/JTC. (2005).

Organización Internacional de Normalización, C. (2008).

Villacis, M. (2016). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001:2013.* Quito.