SISTEMA DE ALERTAS DE SEGURIDAD INFORMÁTICA PARA LOS SERVICIOS CRÍTICOS DE LA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DEL CAUCA (FASE I DEL PROYECTO SGSI-UNICAUCA)

ANDRÉS FELIPE MERA ARCOS
OSCAR EDUARDO MONDRAGÓN MACA

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN
ABRIL de 2012

SISTEMA DE ALERTAS DE SEGURIDAD INFORMÁTICA PARA LOS SERVICIOS CRÍTICOS DE LA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DEL CAUCA (FASE I DEL PROYECTO SGSI-UNICAUCA)

ANDRÉS FELIPE MERA ARCOS
OSCAR EDUARDO MONDRAGÓN MACA

Documento Final de Trabajo de Grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director
Ing. SILER AMADOR DONADO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN
ABRIL de 2012

AGRADECIMIENTOS

Andrés Felipe Mera Arcos expresa sus agradecimientos a:

A mí amada familia por siempre apoyarme en cada paso de mi vida. A mi querida madre Magdalena Arcos por ser la autora de mis grandes triunfos y estar a mi lado en cada derrota. A mi padre Adolfo Mera por darme esos sabios consejos de vida que hoy y siempre aplicaré. A mi hermano Juan Pablo Mera por demostrarme que en la vida se puede lograr lo que se quiere aunque muchos digan que no, ahora sabemos que si podemos.

Al ingeniero Siler Amador Donado por antes que todo ser un buen amigo y excelente maestro, por demostrarme que con pasión y entrega todo se puede lograr.

A mis amigos, mis buenos amigos, por ser los causantes de muchos dolores de cabeza, de locuras y demás, pero ante todo, por ser incondicionales.

Y finalmente a mi siempre amiga y amada Maria Alejandra, por ser el pilar incondicional de mi vida, por ser la persona que siempre está y estará en lo más profundo de mi alma y mente, a ti por ser el motivo real de mi existencia …. Eternal Hailz!!

Oscar Eduardo Mondragón Maca expresa sus agradecimientos a:

A Dios por ser el dueño de mi vida y permitirme cada día visualizar un futuro mejor.

A mi familia por el constante apoyo durante la carrera, a mis padres, Víctor Mondragón y María Eugenia Maca, su ejemplo de responsabilidad y honestidad, mi hermano Víctor por brindar el conocimiento y experiencia en el área de telecomunicaciones, a mis hermanas Claudia por su apoyo incondicional en la universidad y Victoria por siempre estar ahí en los momentos difíciles de realización del proyecto... por ellos y para ellos!

A María Fernanda por ser un punto de apoyo vital en la realización y culminación del proyecto.

Al ingeniero Siler Amador Donado por aceptarme para realizar el presente proyecto de grado, su apoyo, confianza y capacidad para dirigir el desarrollo del proyecto con ideas propias, al igual que el aporte invaluable en mi formación como ingeniero.

A todos aquellos compañeros y amigos que han sido participes de mi vida universitaria generando ideas innovadoras en el campo de la seguridad informática.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

Aceptación del riesgo: decisión de asumir un riesgo.

Activo de información: este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para la empresa.

Amenaza: eventos que pueden desencadenar un incidente produciendo daños materiales o inmateriales a la organización en los activos.

Análisis de riesgos: uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Backups o copias de seguridad: copia de respaldo de la información.

Ciclo Deming: ciclo que incluye las fases planear, hacer, verificar y actuar. Es ampliamente usado para generar control en un sistema.

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

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

Control de seguridad: medida o salvaguardas que se toman para disminuir un riesgo.

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

DNS: servicio de nombres de dominio.

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

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

Impacto: efecto que produce determinado factor sobre algo o alguien.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Riesgo: estimación del grado de exposición de un activo a que una amenaza se materialice sobre él, causando daños a la organización.

Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Servicio: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

SGSI: Sistema de Gestión de Seguridad de la Información. Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Valoración del riesgo: proceso global de análisis y evaluación del riesgo.

Vulnerabilidades: debilidades que tienen los activos que pueden ser aprovechados por una amenaza

RESUMEN

El aporte principal de este trabajo de grado es el desarrollo de un sistema de alarmas de seguridad informática para dos (2) de los servicios críticos en la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca basados en los niveles de riesgo de seguridad de la información.

Se desarrollo un sistema, tomando como base los estándares ISO/IEC 27001:2005[1] e ISO/IEC 27005[2], el cual permita identificar los servicios que presentan mayor nivel de riesgo para así realizarles un tratamiento mediante controles y políticas de seguridad de la información, logrando así una reducción considerable de estos niveles y permitiendo tomar decisiones a futuro que eviten posibles amenazas y vulnerabilidades.

Se hace la aclaración, que a pesar de que el nombre del proyecto en un principio se denominó: “Sistema de Alertas”, por consideraciones propias, y siendo consecuentes con el objetivo buscado, se determinó optar por nombrarlo: “Sistema de Alarmas”, siendo una alarma un estado de acción inmediata y toma de decisiones, por lo que es más acorde al sistema desarrollado.

PALABRAS CLAVE:

- ✓ SGSI
- ✓ Niveles de riesgo
- ✓ Alarmas de seguridad informática
- ✓ Servicios informáticos
- ✓ Amenazas y vulnerabilidades

INTRODUCCION

A diario existen amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información y con ello la viabilidad de los negocios. En la actualidad es indispensable brindar robustez y seguridad a los sistemas de información para así evitar el acceso de personal no autorizado a la red de telecomunicación de las empresas, instituciones, entes gubernamentales, militares y demás organizaciones que utilicen dichos medios para almacenar, procesar y distribuir la información.

La seguridad de la información debe ser tratada con absoluta prioridad por cualquier entidad o empresa que desee estar a salvo de manipulación ilícita o intrusiones no autorizadas.

Por estos motivos es que cada día se realizan nuevas metodologías en busca de mantener a salvo la información. Es el caso puntual de desarrollo de normas y políticas de seguridad como las que emplea los estándares de la familia ISO/IEC 27000. Se tienen en cuenta los estándares ISO/IEC 27001:2005 e ISO/IEC 27005:2008, los cuales usan como núcleo el denominado ciclo Deming (PHVA)[3], el cual muestra el proceso que tiene la información para que garantice su integridad, confiabilidad y disponibilidad. Estos estándares, mediante la implementación de controles y políticas de seguridad, harán posible disminuir las vulnerabilidades y amenazas a las que están expuestos los activos de cualquier empresa.

El caso de trabajo de grado, se encuentra centrado en un sistema de alarmas informáticas en la división de las TIC's[1] de la Universidad del Cauca, que permite medir y reducir los niveles de riesgo en los servicios allí presentes, combatiendo las continuas amenazas que se presentan día a día e identificando las vulnerabilidades que permiten accesos ilícitos o robo de información.

Actualmente están implementados en la División de TIC de la Universidad del Cauca servicios como: WEB, PROXY, DNS, CORREO ELECTRONICO, SIMCA, entre otros, con alto nivel de riesgo, los cuales serán evaluados y clasificados, mediante un instrumento de medición, para obtener dos (2) servicios críticos, a los cuales se les hará un seguimiento para encontrar y corregir las vulnerabilidades de mayor uso por parte de los atacantes o en su defecto, errores internos de dicho servicio, ya sea por una incorrecta configuración por parte del administrador o por factores externos, por ejemplo factores ambientales.

[1] Las tecnologías de la información y la comunicación (**TIC**) agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

Este es uno de los primeros pasos para la construcción de un SGSI (Sistema de Gestión de Seguridad de la Información) para la Universidad del Cauca, el cual permite abrir puertas para el manejo seguro y confiable de la información, y por ende, la estabilidad en los servicios de información prestados por la División de TIC de la Universidad del Cauca.

Para el desarrollo de este trabajo de grado se utilizaron las siguientes metodologías:

- La metodología del Modelo Integral para el Profesional de Ingeniería[4], el cual permite un mejor entendimiento de los objetivos propuestos, hace uso en primera medida del "Modelo para la investigación científica", para generar conocimiento socialmente no existente y que sea útil en el campo de la seguridad informática institucional. Por otro lado, se toma el "Modelo para la construcción de soluciones", cuyo propósito es diseñar y desarrollar un sistema de alarmas de seguridad informática de calidad, óptimo y de costos competitivos.

- La metodología XP[5], la cual permite una planeación y desarrollo del proyecto en forma acertada, haciendo uso de fases de desarrollo planeadas para la consecución de los sistemas específicos, como por ejemplo el instrumento de medición y el sistema de alarmas de seguridad informática.

Con el fin de abordar los temas anteriores y los objetivos requeridos para el desarrollo de este trabajo de grado, el contenido se divide en cinco apartados:

1. Marco teórico
En este apartado se hace énfasis en la parte teórica del proyecto, recolectando la información necesaria y estableciendo las bases para la consecución y desarrollo del sistema.

2. Metodología experimental
Se enfoca en la elaboración de las fases necesarias para el desarrollo de un SGSI en la Universidad del Cauca, teniendo puntos de investigación en el área de trabajo de la División de TIC de la Universidad del Cauca, desarrollo del instrumento de medición y obtención de la criticidad de los servicios evaluados, y finalmente el diseño y desarrollo del sistema de alarmas de seguridad informática para dos (2) de los servicios críticos de la División de TIC de la Universidad del Cauca.

3. Análisis de resultados
Se realiza el análisis de los resultados que se obtuvieron en el transcurso del proyecto y el desarrollo de pruebas de evaluación de funcionalidad en el sistema.

4. Conclusiones, recomendaciones y trabajos futuros

Se detallan una serie de conclusiones que se obtienen de todo el análisis del proyecto y la manera en que se desarrolló. De igual manera se detallan unas recomendaciones sobre el proyecto y los posibles trabajos futuros que se pueden desarrollar a partir del proyecto propuesto.

5. Bibliografía

Se detallan las referencias bibliográficas utilizadas en la investigación y desarrollo de este proyecto de grado.

OBJETIVO GENERAL Y ESPECIFICOS

OBJETIVO GENERAL

Desarrollar un sistema de alarmas de seguridad informática para dos de los servicios críticos en la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca basados en los niveles de riesgo de seguridad de la información.

OBJETIVOS ESPECÍFICOS.

- Adaptar las fases necesarias para el desarrollo del SGSI en la Universidad del Cauca, con base en el estándar ISO /IEC 27001.

- Identificar los servicios críticos y medir los niveles de riesgo de seguridad de la información, con base en el estándar ISO/IEC 27005.

- Diseñar y desarrollar un sistema de alarmas informáticas para dos de los servicios críticos de la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca.

- Evaluar el desempeño del sistema de alarmas informáticas para dos de los servicios críticos de la División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca.

1. MARCO TEÓRICO.

1.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

A diario, los negocios y empresas están expuestos a constantes riesgos y amenazas, a través de diferentes vulnerabilidades, que ponen en peligro los diferentes activos de la información y con ello el progreso de la organización.

Los riesgos y amenazas en muchos casos no solo afectan a la empresa desde el exterior, sino también desde su interior, por eso, se debe brindar confidencialidad, integridad y disponibilidad de la información al establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)[6].

Un SGSI es una herramienta de gestión que permite identificar, gestionar y reducir los posibles riesgos que a diario se presentan sobre los activos de información importantes de toda empresa.

Antes que nada, es importante diferenciar entre seguridad informática y seguridad de la información.

La seguridad informática se centra en proteger los servicios tecnológicos de la información y comunicación (hardware y software) que soportan la empresa.

En cambio, seguridad de la información, se refiere a la protección de los activos de información que se consideran fundamentales por la empresa para la viabilidad del negocio. Ejemplos de esta información fundamental en las empresas son: bases de datos, imágenes, páginas web, correos electrónicos, faxes, presentaciones, documentos, entre otros.

Cuando se logran identificar estos activos de información, se debe tener presente que estos pueden proceder de distintas fuentes dentro de la misma organización y que pueden encontrarse alojados en diferentes medios como físicos (papel) o digitales (CD, DVD, USB, Disco Duro). Además, es fundamental considerar el ciclo de vida de la información, ya que esta puede ser de vital importancia y criticidad hoy pero puede perderla con el tiempo.

La metodología que maneja un SGSI permite analizar y ordenar la estructura de los sistemas de información. También facilita la definición de procedimientos de trabajo para mantener los niveles de seguridad adecuados en la empresa. Y finalmente, ofrece la posibilidad de disponer de controles que permiten evaluar la eficacia de las medidas realizadas.

Las empresas y sus sistemas de información se exponen día tras día a un sinnúmero de amenazas que aprovechan cualquier vulnerabilidad para afectar activos con diversas formas como fraude, espionaje, sabotaje o vandalismo. Son ejemplos comunes los virus informáticos, los ataques de denegación de servicios (DoS)[2] y el denominado "hacking"[3], pero también se deben considerar los continuos riesgos de seguridad causados de forma consciente o no por el personal de la empresa, o fallas técnicas y catástrofes naturales.

Figura 1. Esquema general de tratamiento de riesgos [7].

Con un SGSI, la empresa puede conocer los riesgos a los que se enfrenta y como asumirlos, reducirlos, transferirlos o controlarlos mediante la aplicación de políticas y controles de seguridad, para que así el impacto sea mínimo.

[2] DoS es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
[3] Forma de denominar el acto de entrar a un sistema sin autorización a través de diferentes técnicas sin la aprobación de los usuarios legítimos.

El gestionar los riesgos a través de un SGSI permite mantener en un nivel confiable la integridad, confidencialidad, y disponibilidad de la información, en el interior y exterior de la empresa.

La confidencialidad implica el acceso a la información únicamente por parte de quienes están autorizados, la integridad pretende que la información no se le realice modificaciones no autorizadas, y la disponibilidad indica que la información debe encontrarse accesible para quienes deben o necesitan acceder a ella (personal autorizado, aplicaciones o procesos).

Con el fin de unificar y normatizar diferentes parámetros de seguridad de la información, se han creado un conjunto de estándares bajo el nombre de ISO/IEC 27000. Estas normas permiten disminuir considerablemente el impacto de los riesgos sin necesidad de realizar grandes inversiones en aspectos software y sin contar con una gran estructura de personal.

1.2 ISO/IEC 27001:2005

La seguridad de la información, según el estándar ISO/IEC 27001:2005, consiste en el mantenimiento de los tres pilares fundamentales antes mencionados: la confidencialidad, la integridad y la disponibilidad.

El estándar ISO/IEC 27001 define que un SGSI debe estar constituido por los siguientes documentos[4]:

- Alcance del SGSI
- Políticas y objetivos de seguridad
- Procedimientos y mecanismos de control del SGSI
- Enfoque de evaluación de riesgos
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Procedimientos documentados
- Control de Registros
- Declaración de aplicabilidad

Es de gran importancia tener el control de estos documentos y mantenerlos actualizados para brindar un soporte adecuado al sistema y a los participantes del SGSI.

[4] http://www.iso27000.es/sgsi.html#section2c

Este estándar se encuentra basado en el conocido Ciclo Deming o PHVA (Planificar – Hacer – Verificar – Actuar), que permite a la información estar en continuo tratamiento por parte de políticas y controles, tener planes de contingencia sobre amenazas y vulnerabilidades que conllevan a riesgos, actualización periódica de la información y por tal sus políticas, y cómo manejar el riesgo, si se evita, se asume, se transfiere o se minimiza.

- **Planificar:** Se establece el SGSI.
- **Hacer:** Se implementa y se utiliza el SGSI.
- **Verificar:** Se monitoriza y se revisa el funcionamiento del SGSI.
- **Actuar:** Se mantiene y se mejora el SGSI.

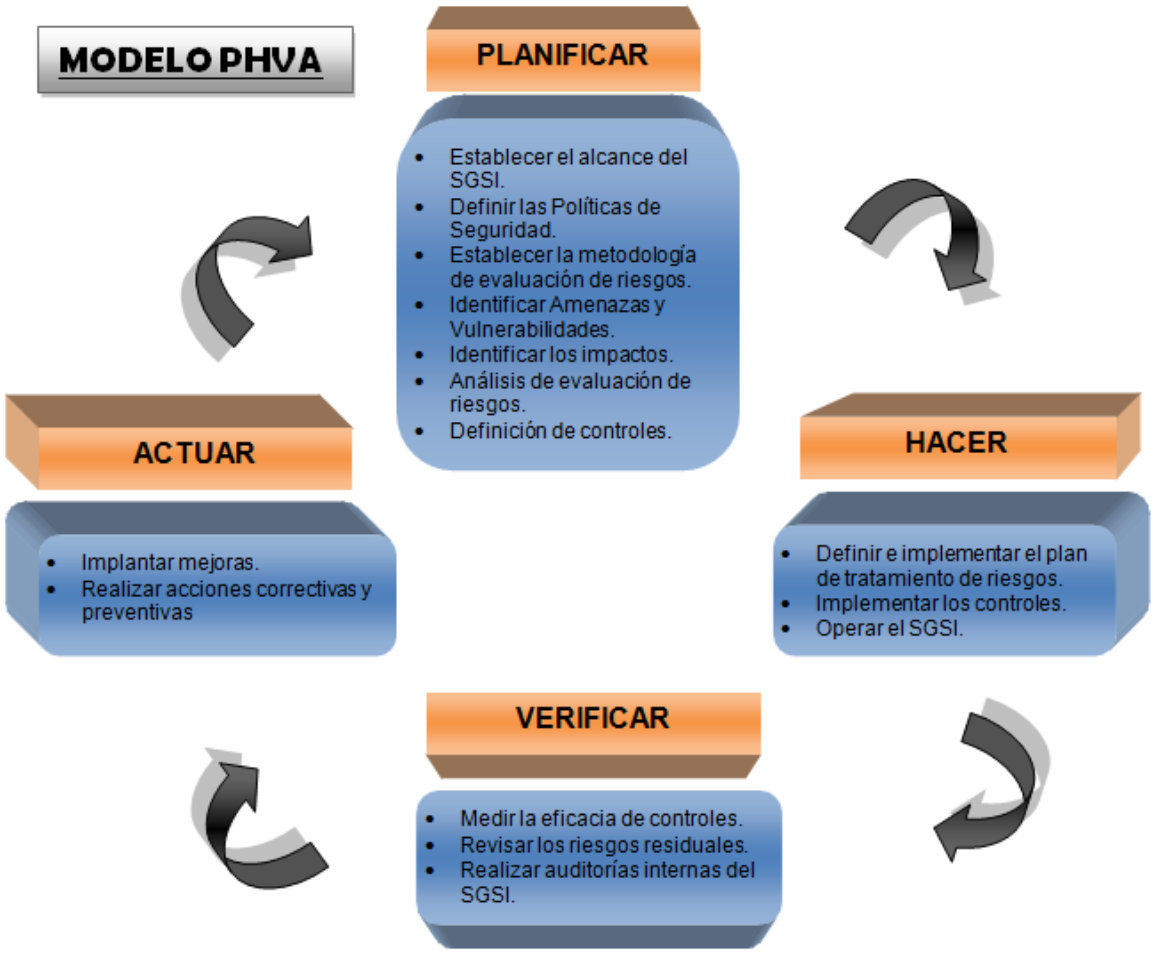


Figura 2. Esquema PHVA.

A continuación una explicación más detallada del proceso PHVA y cómo afecta la efectividad del SGSI.

1.2.1 Planificar.

En este punto se establece el alcance del SGSI dependiendo de los términos del negocio, los activos y tecnologías presentes.

Se deben definir las políticas de seguridad que satisfagan las necesidades y cubran posibles amenazas y vulnerabilidades. Estas deben incluir el marco general y los objetivos de seguridad de la información de la organización, requerimientos legales relativos a la seguridad de la información, deben estar alineadas con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y se mantendrá el SGSI, y finalmente que establezca los criterios pertinentes con que se evaluara el riesgo.

También se debe definir una metodología de evaluación de riesgo acorde a las necesidades del negocio y del SGSI, además de establecer los criterios de aceptación del riesgo y especificar los niveles aceptables de este mismo.

En la identificación de riesgos se deben esclarecer los activos de información que se encuentran dentro del alcance del SGSI y el personal que está directamente encargado de ellos. Se deben identificar las vulnerabilidades que pueden ser aprovechadas por las diferentes amenazas. Finalmente, se identifica el impacto en la confidencialidad, integridad y disponibilidad de los activos de información.

En el análisis y evaluación del riesgo se evalúa el impacto en el negocio debido a algún fallo de seguridad que conlleve a la pérdida de confidencialidad, integridad o disponibilidad de un activo de información. En esta parte se deben estimar los niveles de riesgo y determinar si este riesgo es aceptable o necesita ser tratado.

Así cuando ya se ha identificado el riesgo, sus causas y repercusiones, se pueden aplicar diferentes controles que lo mitiguen, o por el contrario, lo reduzcan a un nivel aceptable mientras este no afecte la continuidad del negocio. También se puede evitarlo o transferirlo a terceras personas, como compañías aseguradoras.

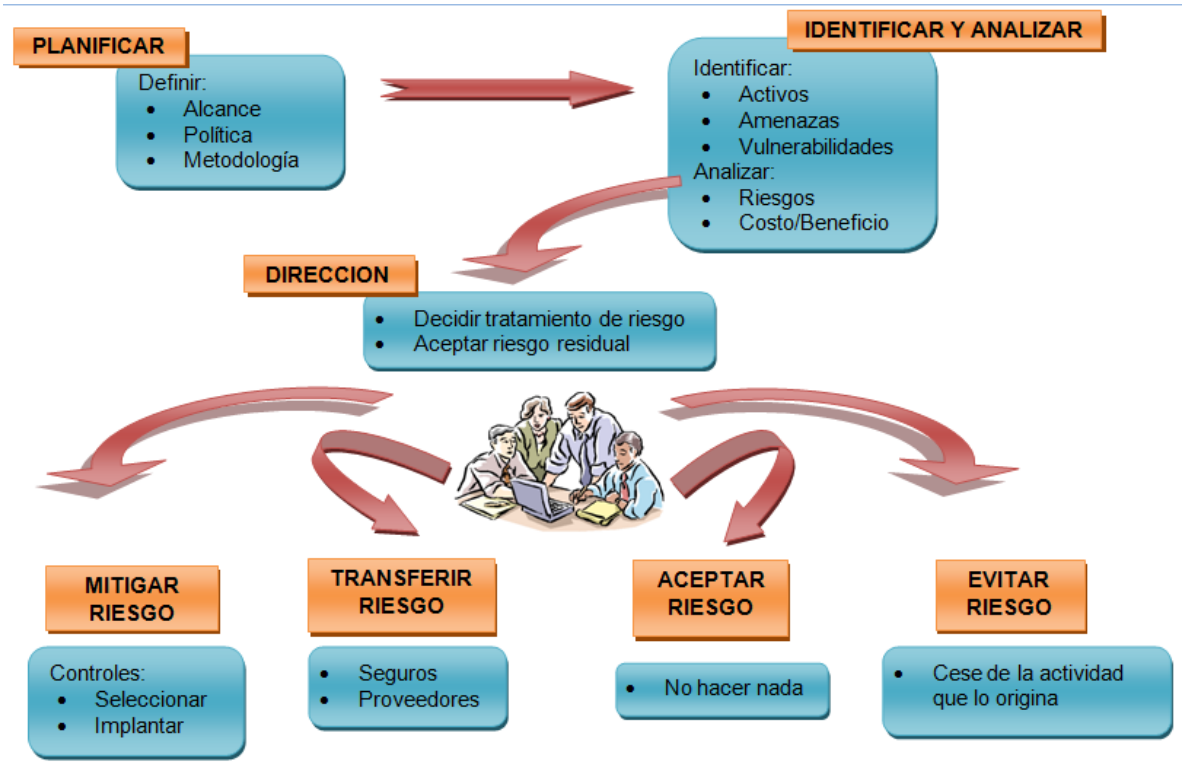


Figura 3. Gestión de riesgos.

Para estos objetivos de control y controles se hace uso del anexo A del estándar ISO/IEC 27001, el cual provee una serie de controles y pautas que permiten realizar el tratamiento adecuado sobre el riesgo y evitar su materialización.

Por lo anterior, es de importancia hacer referencia también en el estándar ISO/IEC 27002:2005[8] (antigua ISO 17799[9]), el cual proporciona un guía completa de implantación de 133 controles. Esta norma es importante ya que es la base para el estándar ISO/IEC 27001:2005.

1.2.2 Hacer.

En este punto se debe definir un plan de tratamiento de riesgos que identifique todas las acciones, responsabilidades y prioridades en la gestión de los riesgos de la seguridad de la información.

Al lograr esto, se debe implantar el plan buscando con ello alcanzar todos los objetivos de control que se han identificado. Así, se implementan los controles que han sido seleccionados minuciosamente para mitigar el riesgo.

Establecido esto, el siguiente paso es definir el sistema de medición de riesgo el cual permita obtener resultados tangibles y comparables para así medir la eficacia de los controles implementados.

Finalmente, se debe buscar la capacitación del personal con el fin de minimizar errores humanos.

1.2.3 Verificar.

En esta sección la organización deberá ejecutar procedimientos de monitorización y revisión, con el fin de detectar a tiempo los diferentes errores que surjan día a día, identificar posibles incidentes de seguridad, medir el trabajo del personal con relación al SGSI, detectar y prevenir incidentes de seguridad mediante el uso de indicadores como por ejemplo un sistema de alarmas.

También se debe revisar regularmente la efectividad del SGSI y la evaluación del riesgo, con el fin de observar si las políticas implantadas están funcionando correctamente o necesitan ser actualizadas, o si los controles están disminuyendo los niveles de riesgo satisfaciendo las necesidades de la organización.

Por todo esto, es conveniente realizar auditorías internas del SGSI con el fin de evaluar el correcto funcionamiento por parte de entes capacitados en el tema.

1.2.4 Actuar.

En esta última fase, la organización deberá regularmente implantar en el SGSI las diferentes mejoras que se van identificando, realizar diferentes acciones preventivas y correctivas que se identifican en la clausula 8 del estándar ISO/IEC 27001:2005 y las propias lecciones aprendidas, con el fin de prevenir posibles fallos.

Todas estas mejoras y acciones se deben comunicar a todas las partes interesadas con el fin de obtener eficacia en el tratado del SGSI.

Este es el ciclo continuo PHVA, el cual indica que después de una fase de *Actuar* lleva de nuevo a la fase inicial de *Planificar* y así sucesivamente. El orden establecido no es estricto y puede modificarse según las necesidades de la empresa.

Es importante resaltar que el compromiso de la empresa es fundamental para el éxito del SGSI. No se debe caer en el error de considerar al SGSI como una cuestión puramente

técnica o tecnológica relegada a niveles inferiores, sino que se debe asumir como parte primordial de la seguridad de la empresa.

La empresa u organización tiene la responsabilidad de definir un alcance aceptable y qué recursos van a destinar para la implantación del SGSI, además de la iniciativa de la aplicación de controles y políticas de seguridad, y como tratar el riesgo que se genera en el transcurso continuo del negocio.

1.2.5 Objetivos de Control

Como se hizo referencia, el estándar ISO/IEC 27001:2005 cuenta con 11 dominios, 39 objetivos de control[5] y 133 controles de seguridad registrados en el anexo A de esta misma. Estos son aquellos que se van a evaluar periódicamente cuando se implante el SGSI. Detrás de cada control se encuentran una serie de políticas y procedimientos de seguridad[6], así que es de gran importancia sentar buenas bases para la correcta funcionalidad del sistema.

Este estándar está ligado fuertemente a la antigua norma ISO/IEC 17799, en la cual se detallan con mayor profundidad los 133 controles.

Los controles no son exhaustivos y la organización pude seleccionar los que se adapten más a sus necesidades. En todo caso, el éxito del SGSI radica en el compromiso y seriedad de la organización para con el sistema.

El anexo está dividido en los siguientes numerales:

- A.5 Política de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Gestión de activos
- A.8 Seguridad de los recursos humanos
- A.9 Seguridad física y ambiental
- A.10 Gestión de comunicaciones y operaciones
- A.11 Control de acceso
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información
- A.13 Gestión de incidentes de seguridad de la información

[5] Objetivo de Control es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática y sistemas de información.

[6] Conjunto de reglas y acciones que permiten el mantenimiento de cierto nivel de seguridad en diferentes ámbitos de trabajo.

- A.14 Gestión de la continuidad del negocio
- A.15 Cumplimiento

Cada numeral se extiende en diferentes secciones, donde no solo se centra en las tecnologías de la información, sino también en la protección legal, asuntos organizacionales, seguridad física, gestión de recursos humanos, entre otros. Estos controles ayudarán a minimizar los riesgos presentes en la empresa y servirán de medida para la evaluación del funcionamiento del sistema.

1.3 ISO/IEC 27002:2005

El estándar ISO/IEC 27002:2005 es una guía de buenas prácticas en la cual se describen los objetivos de control y controles enunciados anteriormente en el anexo A del estándar ISO/IEC 27001:2005, los cuales son recomendados en el área de seguridad de la información. Esta contiene 39 objetivos de control y 133 controles, reunidos en un total de 11 apartados los cuales se enunciaron en el apartado 1.2.5.

La finalidad de esta norma es brindar a la empresa una seguridad total en el momento de la elección de los controles para aplicarlos en el SGSI. Esta, a diferencia del estándar ISO/IEC 27001:2005, no es certificable.

1.4 ISO/IEC 27005:2008

El estándar ISO/IEC 27005:2008 es un estándar que se involucra en el análisis de riesgos de la información, brindando un conjunto de pautas y directrices mediante las cuales la empresa puede realizar un mejor control de los activos de información de la misma.

Se debe señalar que este estándar no brinda una metodología concreta o específica para el análisis de riesgo, sino que describe, a través de las diferentes clausulas que contiene, los procesos recomendados para el correcto análisis. En otras palabras, es utilizada como guía para no tener duda sobre los elementos que debe incluir una correcta metodología de análisis de riesgo. Las fases que contiene este estándar son:

- Establecimiento del contexto (Cláusula 7)
- Evaluación del riesgo (Cláusula 8)
- Tratamiento del riesgo (Cláusula 9)
- Aceptación del riesgo (Cláusula 10)
- Comunicación del riesgo (Cláusula 11)
- Monitorización y revisión del riesgo (Cláusula 12)

Este estándar también incluye seis anexos de carácter informativo (no normativo) que orientan a la empresa en campos como la identificación de activos e impactos, vulnerabilidades y amenazas asociadas a estos activos, y diferentes aproximaciones de análisis de riesgo de la información.

En la figura 4 se muestra el proceso básico de análisis e impacto de riesgo:

Figura 4. Análisis e impacto de riesgo [10].

Todo parte de las necesidades de seguridad de cada empresa, por ende se busca estar protegido ante cualquier eventualidad que pueda comprometer los bienes más preciados, como por ejemplo los activos de información.

Cada día surgen vulnerabilidades que son aprovechadas por las amenazas presentes en todo ámbito empresarial, por consiguiente es necesario implementar un método de contramedida o salvaguardas[7] que satisfaga las necesidades primarias o importantes para el negocio.

Como ya se dijo, los activos de información son los principales afectados por estas vulnerabilidades y amenazas, por lo que se va a generar un impacto en la empresa el cual se debe reducir al máximo posible evitando así que repercuta gravemente en la

[7] Una salvaguarda o contramedida es cualquier método o técnica que ayude a detener las amenazas sobre los activos de información.

continuidad del negocio. Es aquí donde el estándar brinda unos campos de acción para analizar el riesgo y llevarlo a niveles reducidos mediante la correcta aplicación de políticas y controles establecidos por los otros estándares.

En la figura 5 se presenta el proceso sugerido por el estándar para el análisis y gestión del riesgo:

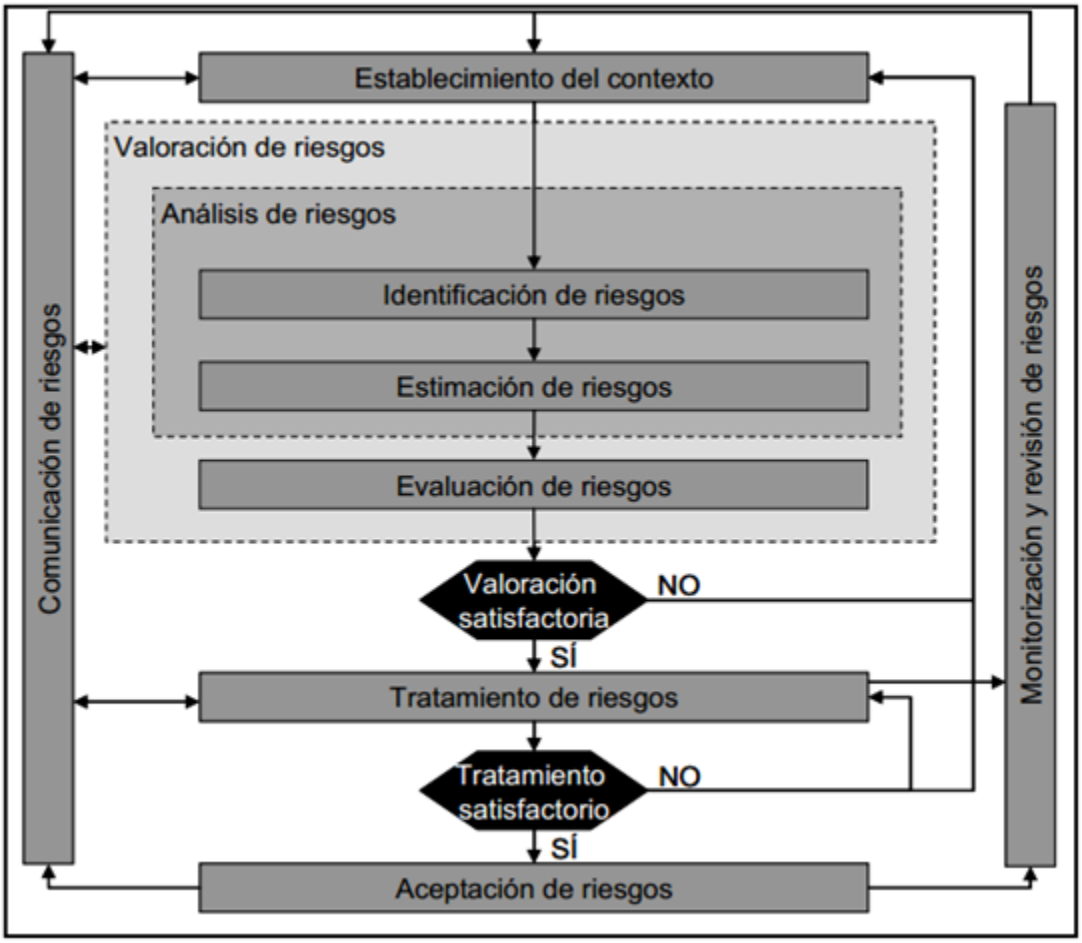


Figura 5. Proceso de gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008 [11].

La catalogación del riesgo se realiza tanto de manera cuantitativa como cualitativa dándole diferentes valores de impacto sobre cada activo. Un activo puede analizarse de manera cuantitativa estableciendo unos niveles de criticidad, como por ejemplo de 1 a 5, siendo 1 el nivel más bajo de impacto de riesgo y 5 el nivel más crítico.

También se tiene en cuenta la parte cualitativa del activo de información, donde se analiza su valor económico, siendo también muy importante el nivel apreciativo de cada uno de ellos para la empresa. Igualmente se puede catalogar mediante niveles o rangos de importancia.

1.5 NAGIOS

Nagios[12] es una herramienta de monitoreo de redes, servicios y equipos que fue concebido para tener control por parte de los administradores de la red la cual administran y así conocer eficientemente los diversos problemas que ocurren en la infraestructura garantizando un grado de disponibilidad de los servicios y equipos.

Nagios es un software libre bajo licencia GPL[8] que se ha diseñado para operar bajo sistemas Linux[9] y es flexible en el momento de adaptar diferentes controles o plugins dedicados a mejorar casos puntuales.

Se reconoce por que hace uso del protocolo SNMP[10] (Simple Network Management Protocol), el cual es un protocolo que permite el manejo seguro de dispositivos de red. Es comúnmente utilizado para monitorear el estado de enrutadores, servidores y otros dispositivos hardware de la red, pero también se puede usar para controlar los dispositivos de la red y enviar avisos o alertas mediante páginas web o correo electrónico cuando suceda un incidente o falla.

Nagios maneja la siguiente estructura:

- Posee un núcleo de la aplicación el cual es la parte lógica de control la cual contiene el software necesario para realizar las tareas de monitoreo de los servicios y las diferentes maquinas de la red.

- Para el despliegue de resultados hace uso de una interfaz web a través de un conjunto de CGI's[11] y de un conjunto de paginas HTML que vienen incorporadas y permiten al administrador una completa visión del qué ocurre, donde y en algunos caso, por qué.

[8] General Public License.
[9] Es un núcleo libre de sistema operativo basado en Unix.
[10] http://net-snmp.sourceforge.net/
[11] Common Gateway Interface o Interfaz de Entrada Común es una importante tecnología de internet permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web.

- Por último, Nagios guarda sus datos históricos en una base de datos para que no ocurra perdida de información al momento en que se detenga y se inicie un servicio.

En la figura 6 se presenta la estructura de Nagios:

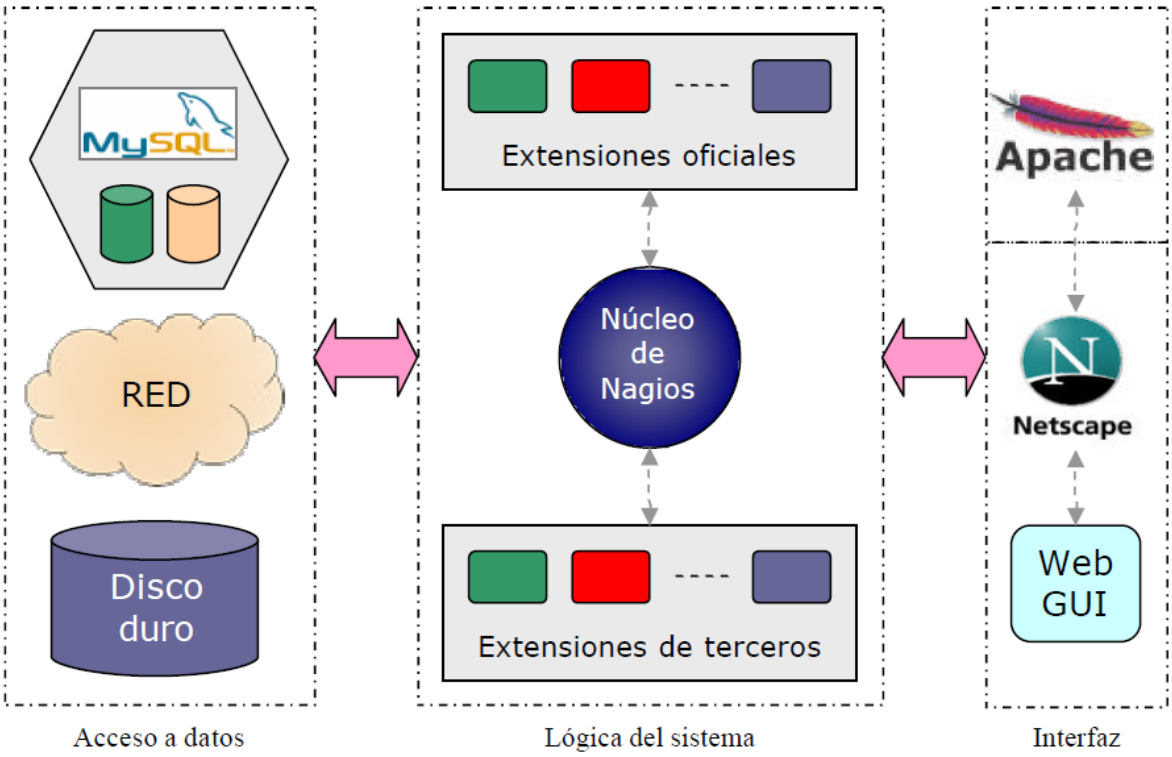


Figura 6. Estructura del sistema de monitoreo Nagios [13].

Algunas características del sistema de monitoreo Nagios son:

- Monitorización de servicios de red: SMTP[12], POP3[13], HTTP[14], SSH, DNS, entre otros.
- Monitorización de recursos: carga de procesador, espacio libre en filesystems, uso de la memoria, entre otros.
- Capacidad de desarrollar plugins de forma sencilla que permite a los administradores manejar el sistema de forma flexible.

[12] Simple Mail Trasnfer Protocol.
[13] Post Office Protocol.
[14] Hypertext Trasnfer Protocol.

- Capacidad de definir diferentes topologías o jerarquía entre dispositivos para identificar servicios o equipos con fallas de los que no.
- Envió de alertas o notificaciones mediante correo electrónico o mensaje de texto al administrador del servicio.
- Consola web de visualización del estado actual de todos los servicios y equipos monitoreados.
- Soporte de base de datos para el almacenamiento de datos externos.

Nagios aplica en el presente proyecto sirviendo como variable complementaria al cálculo de la probabilidad total según el servicio previamente definido como crítico en la División de TIC de la Universidad del Cauca.

1.6 SERVIDORES Y SERVICOS INFORMÁTICOS DE LA UNIVERSIDAD DEL CAUCA[15]

Se pretende enunciar de forma corta y concisa los servicios y servidores pertenecientes a la División de TIC de la Universidad del Cauca, esto con el fin de ampliar el panorama de las tecnologías y brindar un conocimiento sobre los activos de información que se evalúan en este proyecto.

1.6.1 Servicio WEB

Se conoce como Portal Web Institucional de la Universidad del Cauca[16] al sitio de acceso a la información relacionada con hechos sociales, académicos, políticos, entre otros, de la institución universitaria, orientada a informar a la comunidad de la misma como a personas externas. Este sitio está regido por un manual de medios de comunicación el cual permite establecer las conductas y políticas de divulgación de la información.

El servicio debe estar disponible las 24 horas del día y debe brindar información confiable y segura, por lo que es de gran importancia estar monitoreándolo para evitar ataques de denegación de servicio, riesgo de la integridad de la información, acceso no autorizado, entre otros.

1.6.2 Servicio CORREO ELECTRONICO

Es el servicio que permite la emisión de correos electrónicos institucionales mediante la creación de una cuenta con identificación de usuario y contraseña. Cabe resaltar que para

[15] ftp://jano.unicauca.edu.co/AcreInst/DocInfo/Factor8/C24/24A2/DIVISION%20DE%20SISTEMAS/
[16] www.unicauca.edu.co

la creación de una cuenta se debe pertenecer a la institución en cualquier rol y acercarse a las oficinas de contacto 55.

Es de vital importancia brindar integridad, confidencialidad y disponibilidad en el servicio para un correcto desarrollo de las actividades. Pueden existir diversos ataques como por ejemplo la suplantación de identidad, por ende es necesario dar un soporte estable y confiable a este servicio.

1.6.3 Servidor DNS

En la actualidad la Universidad del Cauca posee dos tipos de servidores DNS que permiten la resolución de nombres de dominio: estos son los servidores DNS internos y los externos.

Los servidores DNS externos están capacitados para resolver las direcciones IP públicas que son asignadas a la Universidad, como también atienden las solicitudes de resolución externas a la intranet de esta misma. En cuanto a los servidores DNS internos, estos tienen la tarea de resolver direcciones IP privadas que son asignadas internamente, como también atender las peticiones de resolución externas de los sistemas de cómputo de la intranet de la Universidad del Cauca.

1.6.4 Servidor PROXY

Este servicio es ofrecido buscando el acceso a internet desde cualquier computador que esté ubicado dentro del campus universitario y que posea una conexión a la red de datos. Provee acceso a la web, ftp, servicio de correo electrónico, entre otros. Permite igualmente el control de acceso a diferentes sitios por parte de los administradores del servicio según las políticas de la Universidad del Cauca.

1.6.5 Servicio SIMCA

Sistema Integrado de Matricula y Control Académico (SIMCA)[17] es un portal institucional de la Universidad del Cauca dedicado a la implementación de matriculas académicas de los estudiantes de pregrado. Al igual, provee información sobre el estatus del estudiante, su historia académica, su estado de deudas.

Es muy importante la seguridad de este servicio debido a la información manejada, como por ejemplo las notas académicas de cada estudiante. Sería un gran problema de

[17] Sistema Integral de Matriculas y Control Académico. Se encuentra en el siguiente enlace: https://simca.unicauca.edu.co/simca/

seguridad de la información si personas externas a la Universidad o no autorizadas tuviesen control de este servicio, ya que esto conllevaría a una posibilidad de fraude académico entre otras posibilidades.

2. METODOLOGÍA EXPERIMENTAL.

2.1 FASES NECESARIAS PARA EL DESARROLLO DEL SGSI DE LA UNIVERSIDAD DEL CAUCA CON BASE EN EL ESTANDAR ISO/IEC 27001.

Las fases para el desarrollo de un sistema SGSI son necesarias ya que permiten trazar una guía de procesos los cuales incluyen la identificaciones de los diferentes objetivos de control y controles, sugeridos por el estándar ISO/IEC 27001:2005, presentes en la División de TIC, para así abordarlos de manera confiable.

Estas fases están seriamente ligadas con las fases del ciclo Deming (PHVA), mencionado con anterioridad, por lo que se busca remitirse a él y seguir sus lineamientos aplicándolos de manera explícita en la División de TIC de la Universidad del Cauca para poder generar un procedimiento o plan de tratamiento del SGSI.

2.1.1 Identificación de los objetivos de control en la División de TIC de la Universidad del Cauca.

Mediante la identificación de los diferentes objetivos de control presentes en la División de TIC, se buscó realizar un análisis concienzudo que permitiera observar el comportamiento de dicha área, y a la vez observar las posibles vulnerabilidades que pueden ser aprovechadas por terceros y generar por ende riesgo en los activos de la información.

Esta identificación se llevó a cabo realizando una visita técnica a las instalaciones de la División de TIC de la Universidad del Cauca, en la cual se entrevistó a los ingenieros Alexis Solarte y Fabián Andrés Mera, siendo este último el encargado del área de servidores de la misma. Se buscó mediante el desarrollo de una lista de chequeo, identificar dichos objetivos tomando como base los ya mencionados en el anexo A del estándar ISO/IEC 27001:2005.

En el anexo A tabla A.1 de este trabajo de grado se podrá encontrar la lista de chequeo realizada que permitió identificar los controles implementados por parte de la Universidad del Cauca. Aunque se han implementado algunos controles y políticas, muchos de estos no se encuentran estandarizados por una norma legal o se encuentran en fase de desarrollo, por lo que es necesaria su pronta implementación para así poder disminuir el riesgo en los activos de la información.

2.1.2 Clasificación de los objetivos de control encontrados en la División de TIC de la Universidad del Cauca.

Con base al estándar ISO/IEC 27001:2005 se procedió a realizar el análisis y clasificación de los objetivos de control presentes en la División de TIC de la Universidad del Cauca con el fin de observar de manera crítica y profunda las necesidades presentes en el área.

Esta clasificación fue importante porque permitió acercarse más hacia las necesidades de la institución y poder definir así los objetivos de control necesarios para brindar seguridad de la información a los activos presentes en la misma.

En el anexo A tabla A.2 se consignan los resultados obtenidos después de realizar la clasificación. Para este punto se tuvo el soporte del ingeniero Fabián Mera encargado del área de servidores de la División de TIC de la Universidad del Cauca.

2.1.3 Investigación sobre las plataformas de gestión presentes en la División de TIC de la Universidad del Cauca.

Con el fin de aprovechar al máximo las diferentes fuentes de gestión existentes en el mercado, se procedió a realizar una lista de chequeo la cual permitiera indagar sobre las plataformas de gestión o herramientas presentes en el a División de TIC de la Universidad del Cauca. Esto se hizo con el fin de analizar las posibilidades de asociación de estas con el sistema propuesto en este trabajo de grado, y de igual manera poder tener la certeza y la seguridad de que el desarrollo propuesto no existe o no esta implementado en esta área a través de otra herramienta.

Se procedió a realizar una visita técnica a las instalaciones donde se pudo observar una plataforma que integra varias herramientas del mercado como por ejemplo: Nagios, AWstats[14], SARG[15], FortiGate[16], NetXplorer,[17] entre otros. Estos son asignados para funciones específicas dependiendo el tipo de servicios que atiendan o supervisen. Según esto, se realizó una lista de chequeo en la cual fue entrevistado nuevamente el ingeniero Fabián Mera.

En el anexo A – tabla A.3 se puede encontrar la lista de chequeo realizada donde se indaga sobre estas herramientas y las funcionalidades que prestan.

2.1.4 Recopilación de información que aporte a la construcción del sistema SGSI.

Se realizó la búsqueda de información importante que orientara un poco más hacia la identificación de las fases del sistema de gestión y la construcción del mismo SGSI.

Se encontraron fuentes de información en diferentes documentos virtuales y tesis de grado los cuales estaban alojados en las respectivas bases de datos universitarias.

Esta búsqueda permitió acercarse un poco más a conocer la verdadera aplicación de un SGSI en diferentes áreas comerciales y corporativas. En cuanto a la aplicabilidad, se observó que solo se llega a una etapa de estudio y de identificación de riesgos en activos de información, mas no se enuncia una etapa de desarrollo de herramientas de gestión basados en estándares como la desarrollada en este trabajo de grado.

La explicación y evaluación de esta información se realiza en el numeral 2.1.5 con el fin de compilar la información final.

2.1.5 Evaluación de los recursos críticos encontrados en las plataformas de gestión y las tesis evaluadas.

En esta etapa de identificación y clasificación de información se procedió a realizar una evaluación de los recursos críticos presentes en las herramientas de gestión de la División de TIC de la Universidad del Cauca y como pueden ser aprovechadas por este proyecto.

De igual manera se realizó una tabla de análisis de la información recolectada mediante la investigación, esto, como ya se dijo, para fortalecer las bases de conocimiento y poder mejorar el sistema.

Esta es la etapa concluyente de identificación para poder desarrollar las fases necesarias para la implementación del SGSI de la Universidad del Cauca.

En el anexo A – tabla A.4 se muestra la tabla comparativa donde se realiza la evaluación de los recursos de información nombrados que fueron relevantes para este proyecto.

2.1.6 Fases finales para el desarrollo del SGSI de la Universidad del Cauca.

Se presentan a continuación las fases necesarias para la implantación de un SGSI en la Universidad del Cauca basándose en el ya enunciado estándar ISO/IEC 27001:2005 y en las fases o etapas del ciclo PHVA:

- **ETAPA I: Planificar.**

  Fase 1. Establecer la política de seguridad y el alcance del SGSI. La política de seguridad de la información son las instrucciones gerenciales que especifican el camino por el cual se debe manejar un problema o situación. Dicha política de seguridad en la organización se debe definir en términos de las características de la organización, su contexto, tecnología y ubicación.

  Se debe definir de forma clara el alcance del sistema de gestión de seguridad de la información sin perder de vista el enfoque principal de la organización, prioridades de la dirección, relación directa con las actividades de la organización.

  En el momento de la construcción de las políticas del SGSI se debe acudir a:

  - ✓ Asesoría de la dirección.
  - ✓ Comunicación apropiada.
  - ✓ Naturaleza de la organización.
  - ✓ Gestión del riesgo.
  - ✓ Implementación de controles.

  Fase 2. Identificación de los activos: amenazas, vulnerabilidades y riesgos. La identificación de los activos es parte fundamental en la implementación de un sistema de gestión de la seguridad de la información al ser el ente fundamental de toda organización. Pueden existir miles de activos en una organización, pero es importante tener claro el alcance del SGSI y así poder asociar que activos se ven comprometidos realmente con la labor primordial de la organización.

  Los activos de la organización tienen diferentes tipos de clasificación como por ejemplo: por áreas a las que están relacionadas en la organización, por el tipo de activo al que pertenecen, ya sea digital, impreso o conocimiento; clase del activo: informático, tecnológico; activo material o inmaterial.

  Fase 3. Análisis del riesgo. El análisis de riesgo es crucial en un SGSI. Resulta ser una de las fases de mayor importancia ya que es donde se realiza la clasificación cualitativa y cuantitativa de la confidencialidad, integridad y disponibilidad en los activos de información, además se identifican los riesgos asociados con las vulnerabilidades, amenazas y probabilidad de ocurrencia existentes en cada unos de ellos, para así poder identificar el impacto en la organización.

Se debe establecer una metodología para la valoración del riesgo, aceptación y niveles de riesgo aceptable.

Los riegos pueden ser:

- ✓ Mitigados mediante la aplicación de controles apropiados.
- ✓ Aceptarlos con el conocimiento y objetividad, siempre que cumplan con la política de seguridad previamente establecida por la organización.
- ✓ Transferirlos a entidades como aseguradoras, proveedores, siempre que no resulte un costo superior al del riesgo mismo.

Fase 4. Identificar los controles. Los controles se deben seleccionar de manera que cumplan la mitigación de los riesgos encontrados en los activos de la organización, ya sea afectando la probabilidad de ocurrencia o el impacto en la organización según el caso. Los controles del anexo A de la norma ISO 27001:2005 son fundamentales en la implementación de un sistema de seguridad de la información, y la organización debe establecer si necesita adicionar controles en caso de identificar riesgos propios en su enfoque organizacional.

La implementación de controles y la correcta aplicación de activos repercutirán en la adopción de un adecuado nivel de riesgo, compatible con el normal desenvolvimiento de la organización y el coste de las operaciones.

- **ETAPA II: Hacer.** Implementar y operar las políticas de seguridad, controles, procesos y procedimientos.

Fase 5. Gestión del riesgo. Al igual que el análisis de riesgo, la gestión se convierte en un pilar del éxito o no del SGSI. La gestión de riesgo hace referencia a la implementación de los controles seleccionados a través de la metodología expuesta para reducir los niveles de riesgo en base a los umbrales establecidos, para posteriormente realizar una evaluación comparativa entre los niveles obtenidos del análisis y la gestión, y así determinar la efectividad o no de los controles implementados y como afectan el correcto funcionamiento del SGSI.

La implementación de controles resulta ser una laboral de revisión frecuente y por ende se debe verificar el cumplimiento de los siguientes apartados:

- ✓ Los riesgos deben ser mitigados, o en su defecto, estar por debajo del nivel aceptable de la organización.

- ✓ Detección de las violaciones de las políticas de seguridad de la información.
- ✓ Establecer la eficiencia y eficacia de los controles implementados.

Se debe tener en cuenta que el desarrollo de un control de seguridad debe ser, en cuestión económica, menos costoso que el activo de información que va a proteger, y de igual manera, que al atacante que pretenda explotar una vulnerabilidad (suponiendo un ataque de una persona externa a la organización) le resulte extremadamente costoso realizar con éxito dicho ataque.

Es de gran importancia que el personal de la institución posea una capacitación adecuada en el manejo del sistema y de la evaluación de las políticas y controles, ya que de esto de pende su optimo funcionamiento y se eviten riesgos en los activos de la información por la carencia de conocimiento.

Fase 6. Identificar los riesgos residuales. Los riesgos residuales resultan tras la implementación de los controles y es importante identificar aquellos de mayor valor para una posible reevaluación e implementación de nuevos controles que lo mitiguen hasta llevarlo a un nivel de riesgo aceptable, previamente establecido por la organización.

Deben ser aprobados en su totalidad los riesgos residuales de menor valor y monitorearlos con frecuencia de modo que se detecte un aumento en el mismo.

- **ETAPA III: Verificar.**

Fase 7. Monitoreo y revisión del SGSI. Una vez definido y ejecutado el SGSI, resulta importante, después de cierto periodo, una revisión que permita confrontar los datos de la etapa inicial con los actuales, buscando de un modo comparativo, las mejoras y los puntos donde deben emplearse acciones de mejora.

Con el fin de mejorar los niveles de riesgo residual aceptable se deben tener en cuenta los siguientes apartados:

- ✓ Cambios en la organización.
- ✓ Cambios en la tecnología.
- ✓ Cambios en los objetivos de académicos.
- ✓ Cambios en la amenazas.
- ✓ Cambios en las regulaciones externas como regulaciones, leyes.

Es de gran importancia establecer un cronograma de verificaciones del funcionamiento del SGSI, así como procedimientos de monitoreo que buscan la detección de errores, identificación de ataques fallidos y/o exitosos a los servicios informáticos y las diferentes acciones que se realizan con el fin de resolver brechas de seguridad.

Se debe mantener registro de las acciones y eventos que pueden impactar al SGSI ya que esto permitirá realizar acciones de backup[18] o corrección de errores.

Como parte final, se deben realizar revisiones regulares de la eficiencia del SGSI ya que esto permitirá que el sistema este actualizado y brinde la seguridad necesaria.

- **ETAPA IV: Actuar.**

Fase 8. Mantenimiento y mejora de SGSI. La organización debe tomar acciones preventivas, correctivas, lecciones aprendidas; basadas en la fase de monitoreo y revisión de las políticas de seguridad, nuevos activos y los eliminados; con el fin de actualizar los riesgos asociados y posibles controles que los mitiguen. Se debe conocer la eficiencia y eficacia de los controles implementados.

Se deben comunicar los resultados y acciones a emprender, y es necesario tener una buena comunicación con las partes involucradas para tomar decisiones unánimes.

En la figura 7 se presenta un esquema que permite resolver y/o mejorar los requisitos de seguridad de la información:

[18] Copia de seguridad que se realiza con el fin de salvaguardar la información original por si esta se llega a perder, así se puede realizar una restauración de la información.

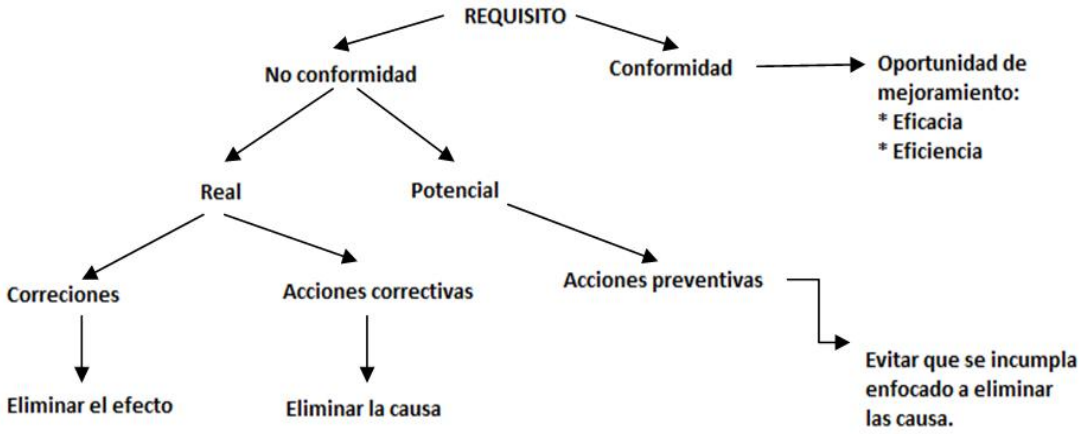


Figura 7. Ciclo de mejoramiento de los requisitos de seguridad de la información.

Fase 9. Documentación. Se puede decir que es una fase de gran importancia ya que permite referenciar todos los procedimientos realizados que afectan directamente al sistema. En esta fase se consignan documentos como guías de seguridad, políticas y controles de seguridad, procesos y actividades de gestión, tareas y requisitos del sistema.

Es importante que se conserve la confidencialidad e integridad de estos documentos debido a que un acceso no autorizado puede significar intrusiones o robo de activos.

De igual manera, es conveniente que se estén actualizando constantemente ya que de esto depende la eficacia del sistema.

2.2 IDENTIFICACIÓN DE LOS SERVICIOS CRÍTICOS Y MEDICIÓN DE LOS NIVELES DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN EL ESTÁNDAR ISO/IEC 27005.

La identificación de los servicios críticos presentes en una organización es de vital importancia ya que permite brindar mayor atención a estos revisando sus niveles de riesgo constantemente, además, que estos pueden ser servicios principales de los cuales se derivan muchos más servicios, por ende es fundamental ser preventivos en el manejo de ellos y reducir o mitigar las amenazas y vulnerabilidades que los asechan.

En este punto se buscó, basándose en el estándar ISO/IEC 27005, una metodología para realizar el análisis de riesgo de la División de TIC de la Universidad del Cauca, que permitiera, como primera medida, identificar los servicios prestados y así poder catalogar la importancia de estos.

Se buscó, no solo tener las especificaciones del estándar ISO/IEC 27005, sino también las sugerencias y recomendaciones de los administradores de los servicios, permitiendo atacar las necesidades primarias de la División de TIC de la Universidad del Cauca.

Todo esto, permitió el desarrollo de una metodología de medición de niveles de riesgos que en este trabajo de grado se denominará “Instrumento de Medición”, el cual cumple la función de realizar el análisis de riesgo, y teniendo diferentes parámetros sugeridos por el estándar, arrojar resultados puntuales que permita identificar los servicios críticos en riesgo.

2.2.1 Servicios informáticos presentes en la División de TIC de la Universidad del Cauca.

En esta fase se procedió a realizar una visita técnica a los administradores de la División de TIC de la Universidad del Cauca, teniendo como objetivo identificar los diferentes servicios prestados, la importancia de cada uno y cómo afecta si dejaran de funcionar.

A través de esta visita técnica se pudo desarrollar una lista de chequeo ubicada en el anexo A – tabla A.5 de este trabajo de grado, en la cual se entrevistó al ingeniero Fabián Mera encargado del área de servidores en la División de TIC de la Universidad del Cauca.

Algunos de los servicios críticos implementados en la División de TIC de la Universidad del Cauca, y que por ser importantes para los administradores del área se deben tener presentes, son:

- Servicio WEB
- Servicio FTP
- Servicio CORREO ELECTRONICO
- Servicio DNS
- Servicio BASE DE DATOS
- Servicio BACKUPS

Algunos servicios, no menos importantes que los anteriores pero que a raíz de su estudio se considero son secundarios o dependientes de otros servicios, fueron:

- Servicio SIMCA
- Servicio de APLICACIONES DE SISTEMAS

La identificación de estos servicios permitió observar de manera más crítica el funcionamiento de estos, la importancia y prioridad que tiene para los administradores y la seguridad que se les presta. Esta última parte es muy importante, ya que es una clara imagen de los procedimientos implementados, como también si existen políticas y controles sobre cada uno de ellos. En caso de no existir, arrojará un alto índice de riesgo y por ende el servicio podrá ser afectado por fallas técnicas o terceros.

2.2.2 Desarrollo del instrumento para la medición de niveles de riesgo.

Se procedió a diseñar y desarrollar un instrumento de medición de niveles de riesgos tomando como base las especificaciones del estándar ISO/IEC 27005. Este instrumento aplica para los diferentes activos de la información siempre y cuando sean medibles.

El análisis del riesgo es crucial en un SGSI, ya que es donde se realiza la clasificación cualitativa y cuantitativa de la confidencialidad, integridad y disponibilidad de los activos de información; se identifican los riesgos asociados con las vulnerabilidades, amenazas y probabilidad de ocurrencia existentes en cada unos de ellos, y así se puede identificar el impacto en la organización.

Los criterios del nivel de riesgo se basaron en:

- ✓ El valor del activo de la información, el cual depende del valor financiero, la criticidad de la confidencialidad, integridad y disponibilidad.
- ✓ La probabilidad de que las amenazas exploten una o más vulnerabilidades de los activos de información.
- ✓ El impacto debido a la explotación de vulnerabilidades por parte de las amenazas.

El método de análisis utilizado en la valoración de riesgos se tomó del estándar ISO/IEC 27005:2008, donde a cada activo se le identifican los riesgos, amenazas o eventos que pueden desencadenar un incidente, vulnerabilidad o debilidad. Dado lo anterior se procedió en la aplicación de la siguiente ecuación que dio como resultado el valor de riesgo en cada activo de información:

Valor Riesgo = P(a,v) * Valor Impacto * Valor Activo (1)

- ✓ *P(a,v)*: probabilidad de ocurrencia de que una amenaza explote una vulnerabilidad.

- ✓ *Valor del Impacto:* está determinado por el responsable del activo de información, quién provee cuanto se vería afectado por incidentes de los activos a cargo.

- ✓ *Valor del Activo:* está determinado por el valor de la confidencialidad, integridad, disponibilidad y el valor económico

El proceso utilizado para el análisis de riesgos de los servicios críticos de la División de TIC de la Universidad del Cauca comprende los siguientes pasos:

- **Identificación de los activos de información de la Universidad del Cauca.** Un activo de información es todo aquello que tiene valor para la División de TIC de la Universidad del Cauca y por tanto necesita protección.

  La identificación de los activos de información se realizó mediante la clasificación por áreas pertenecientes a la Universidad del Cauca, seguido del análisis y determinación de cuales activos de dichas áreas interactúan directa o indirectamente en el alcance definido por la Universidad para el Sistema de Gestión de Seguridad de la Información.

  Existen 2 formas de clasificar los activos:

Tipo de activo	Activos de Información Puros
	Activos Físicos de Tecnologías de Información
	Activos de Información Humano
Clase de activo	Datos Digitales
	Archivos de Información tangibles
	Activos de Información intangibles
	Aplicaciones software
	Software de sistemas operativos
	Software de infraestructura de TI
	Controles ambientales de TI
	Hardware de TI
	Activos de servicios de TI
	Empleados
	No Empleado

Tabla 1. Clasificación de los activos.

- **Cálculo del valor de los activo de información.** El paso que prosiguió tras la identificación de los activos de información en cada área fue definir que variables deben considerarse en el cálculo de estos.

  El valor del activo es determinado por la suma de las siguientes variables:

  - ✓ Confidencialidad
  - ✓ Integridad
  - ✓ Disponibilidad
  - ✓ Valor económico

  La tabla 2 muestra las diferentes especificaciones de los valores que puede tomar cada criterio del valor del activo de información. El rango de valores económicos para los activos de información fueron aproximaciones realizadas en consenso con los administradores de la División de TIC de la Universidad del Cauca.

Confidencialidad – Integridad - Disponibilidad		**Valor económico**		
Muy Alto	5	**$ 50.000.000 +**	Muy Alto	5
Alto	4	**$ 6.000.000 - $ 50.000.000**	Alto	4
Medio	3	**$ 4.000.000 - $ 6.000.000**	Medio	3
Bajo	2	**$ 2.000.000 - $ 4.000.000**	Bajo	2
Muy Bajo	1	**$ 0 - $ 2.000.000**	Muy Bajo	1

Tabla 2. Clasificación del valor del activo según su criterio.

El valor del activo de información está dado por:

$$Valor\ Activo = C + I + D + VrEc \quad (2)$$

La tabla 3 presenta la clasificación final del activo de información y el posible valor que puede tomar dentro de un rango de 4 a 20. Las relaciones entre rangos se realizaron a criterio del proyecto.

	Clasificación	Valor
VALOR DEL ACTIVO	Muy Alto	17-20
	Alto	14-16
	Medio	11-13
	Bajo	7-10
	Muy bajo	4-6

Tabla 3. Clasificación del valor del activo según su valoración.

- **Identificación de las amenazas presentes en los activos de información de la División de TIC de la Universidad del Cauca.** Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas. Algunas amenazas pueden afectar a más de un activo de información generando diferentes impactos.

  La tabla 4 presenta las amenazas identificadas en la División de TIC de la Universidad del Cauca y que fueron usadas en este proyecto de grado:

Amenazas	
Acceso no autorizado	Entidades reguladoras
Avería de origen físico	Errores de monitorización (logs)
Parches desactualizados	Errores de usuarios
Corte de suministro eléctrico	Fallas eléctricas
Daños por agua	Fallo de comunicaciones
Degradación de los soportes principales de almacenamiento de información	Fenómeno natural
Derrame de líquidos o sólidos	Fuego
Difusión de software dañino	Virus informático y software malicioso

Tabla 4. Amenazas.

- **Identificación de las vulnerabilidades presentes en los activos de información de la División de TIC de la Universidad del Cauca.** Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por ciertas amenazas. Una vulnerabilidad que no tiene una amenaza, puede no requerir de la implementación de un control, para lo cual es necesario identificarla y monitorearla, pero es necesario dejar en claro que un control mal diseñado e implementado puede convertirse en una vulnerabilidad.

Se procedió a realizar una lista de chequeo y una encuesta al ingeniero Fabián Mera. Con lo anterior, se buscó observar las medidas de seguridad con que manejan la información en la División de TIC de la Universidad del Cauca para poder llegar a la identificación de las vulnerabilidades en los activos y que amenazas pueden explotar dichas vulnerabilidades. De igual manera este proceso permite evaluar que activos, o en este caso, que servicios poseen un mayor nivel de riesgo y necesitan ser tratados con mayor urgencia.

Algunas de las vulnerabilidades encontradas y utilizadas en este proyecto de grado fueron se encuentran en la tabla 5:

Vulnerabilidades
El periodo de cambio de contraseñas es muy largo
Acceso a los servidores desde equipos de computo personales
Desconocimiento de la política de seguridad de la información
Incorrecta gestión de virus y malware
No hay controles para la actualización de software
Débil control de acceso a los puestos de trabajo
Incorrecta gestión de contraseñas en inicio de sesión de usuario
No hay copias de respaldo

Tabla 5. Vulnerabilidades.

En el anexo A de este trabajo de grado (tabla A.6 y tabla A.7), se pueden encontrar los documentos respectivos.

- **Identificación de los riesgos según las amenazas y las vulnerabilidades.** El riesgo en seguridad de la información es probabilidad de que una o varias vulnerabilidades de los activos de información sean explotadas por una o varias amenaza.

Los riesgos están clasificados por:

Tipo Riesgo
Lógico
Físico
Locativo
Legal

Tabla 6. Tipo de riesgo.

Algunos de los riesgos identificados y utilizados en este proyecto de grado fueron:

Riesgos
Alteración de la información
Denegación del servicio
Fuga de información
Pérdida total de la información
Averías en los equipos
Propagación de los impactos

Tabla 7. Riesgos.

Los riegos se pueden:

- ✓ **Mitigar** mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda revaluar como aceptable.
- ✓ **Aceptar** con el conocimiento y objetividad, siempre que cumplan con la política de seguridad previamente establecida por la organización.
- ✓ **Evitar** la acción que da origen al riesgo particular.
- ✓ **Transferir** a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.

La totalidad de los riesgos identificados en la División de TIC de la Universidad del Cauca, y relacionados a las vulnerabilidades y amenazas de los activos de información, están listados en la matriz de análisis de riesgos ubicada en el anexo A – tabla A.8 de este trabajo de grado.

- **Determinación del impacto en los activos de información de la División de TIC de la Universidad del Cauca.** El impacto es determinado por el responsable de los activos de información de la División de TIC de la Universidad del Cauca, en este caso el ingeniero Fabián Mera, quien determina cuánto daño generaría la materialización de las amenazas sobre las vulnerabilidades de los activos.

  Se hace uso nuevamente de una calificación cuantitativa del impacto, tomando una escala del 1 al 5, siendo 1 un impacto muy bajo y 5 un impacto critico. Para esta valoración del impacto el administrador tiene en cuenta criterios como el monetario, ya que siendo los activos de información servicios institucionales, la no

disponibilidad de uno o más de ellos indicaría o propiciaría pérdidas económicas para la Universidad del Cauca.

	Clasificación	Valor
VALOR DEL IMPACTO	Muy Alto	5
	Alto	4
	Medio	3
	Bajo	2
	Muy bajo	1

Tabla 8. Clasificación del valor del impacto.

- **Determinación de la probabilidad de ocurrencia.** La probabilidad de ocurrencia es la probabilidad de que una amenaza explote una vulnerabilidad en un activo de información, generando un impacto en la empresa y está determinada por la ponderación de dos (2) variables:

Probabilidad Total = [0.30*(Probabilidad A) + 0.70*(Probabilidad B)] (3)

La probabilidad A es determinada por los resultados de la encuesta realizada a los encargados del área de servicios de la División de TIC de la Universidad del Cauca. La encuesta está separada en 3 partes:

- ✓ Seguridad Lógica.
- ✓ Seguridad Física.
- ✓ Seguridad Locativa

La probabilidad B está determinada por los datos obtenidos del sistema de monitoreo Nagios, el cual se encuentra configurado para detectar el cambio de estado y características de ciertos servicios críticos de la División de TIC de la Universidad del Cauca. El sistema de monitoreo Nagios arroja datos confiables para el cálculo de la probabilidad de ocurrencia, es por eso que se le asigna un 70% de credibilidad en contra de un 30% de la encuesta ya que esta se puede acomodar según las necesidades de quien la diligencia, en este caso puntual el administrador del servicio.

Nagios entrega como resultado, tras cada consulta a los servicios gestionados, los posibles datos consignados en la tabla 9:

Dato de Nagios	Descripción
OK	El activo se encuentra en correcto funcionamiento
WARNING	El activo se encuentra en estado de alerta ya que puede superar cierto umbral. El servicio se puede encontrar en un estado UP/DOWN/UNREACHABLE.
CRITICAL	El activo se encuentra inactivo o inalcanzable.

Tabla 9. Estados de respuesta de Nagios.

El sistema de alarmas de seguridad informática toma el valor entregado por el sistema de monitoreo Nagios y asigna un valor cuantitativo de probabilidad para determinar la probabilidad total de que una amenaza explote una vulnerabilidad y se genere un riesgo en un activo de información.

La tabla 10 muestra los valores asignados según el estado del activo de información monitoreado:

Dato de NAGIOS	Valor Cuantitativo
OK	30%
WARNING	60%
CRITICAL	90%

Tabla 10. Valor cuantitativo de los estados de respuesta de Nagios.

Los valores anteriores se asignaron en base a la información proporcionada por el plugin de Nagios denominado *chek_http*[19], en el cual se tiene una valoración de estados con un rango máximo posible de 500, siendo 400 un estado CRITICAL, 300 un estado WARNING y 200 un estado OK.

Con el valor de la encuesta y el valor entregado por el sistema de monitoreo Nagios, se realiza el cálculo de la probabilidad total de cada activo de información.

El cálculo total del valor del riesgo es determinado por la ecuación (1), donde se tiene el valor de los activos de información, el impacto suministrado por el responsable del activo de información y el valor de probabilidad de ocurrencia total.

Existen casos en los cuales un activo de información posee varias vulnerabilidades asociadas a diferentes amenazas generando ciertos riesgos, para ello es

[19] http://nagiosplugins.org/man/check_http

necesario realizar una selección del riesgo identificado como más alto, y es a dicho riesgo que se le aplica las posibles formas de tratamiento.

En la tabla 11 se clasifican los posibles valores que surgen después del cálculo del valor de riesgo a los activos de información:

Clasificación Riesgo	Rango	
Muy Alto	401	500
Alto	301	400
Medio	201	300
Bajo	101	200
Muy Bajo	4	100

Tabla 11. Clasificación del valor de riesgo.

Los valores de riesgo a tratar establecidos como rangos críticos en la División de TIC de la Universidad del Cauca son *Alto* y *Muy Alto*, que corresponden a los siguientes valores:

Alto (301-400) – Muy Alto (401-500)

Los rangos seleccionados fueron escogidos por estar en un alto valor de riesgo e Impacto. La materialización de las amenazas hacia las vulnerabilidades en los activos críticos de información genera graves consecuencias en la organización.

Se considera un valor de riesgo aceptable por la División de TIC de la Universidad del Cauca los siguientes rangos:

Muy Bajo (4) – Medio (300)

Los rangos seleccionados se consideran como valores de riesgo aceptables debido a que está controlada su probabilidad de ocurrencia o su impacto en caso de materializar una o varias amenazas.

De igual forma, se establecen unos rangos por colores en la tabla 12, los cuales indican el nivel de riesgo que se presenta, esto con el fin de facilitar parámetros visuales que indiquen la implementación o no de medidas de control.

Clasificación Riesgo	Rango
Muy Alto	
Alto	
Medio	
Bajo	
Muy Bajo	

Tabla 12. Clasificación del valor de riesgo.

Todo control aplicado con el fin de mitigar el valor de riesgo calculado debe ser medible a través de su eficiencia y eficacia. La aplicación de un control no necesariamente implica la reducción total del valor de riesgo esperado sino la reducción a los niveles de riesgo aceptables establecidos por la organización, en este caso la División de TIC de la Universidad del Cauca.

La funcionalidad de los controles debe ser constantemente evaluada; en caso de no obtener los resultados esperados se les deben aplicar las mejoras a través de una nueva aplicación de la metodología PHVA.

2.3 DISEÑO DE UN SISTEMA DE ALARMAS DE SEGURIDAD INFORMÁTICA PARA DOS (2) DE LOS SERVICIOS CRÍTICOS DE RIESGO DE LA INFORMACIÓN PRESENTES EN LA DIVISIÓN DE TIC DE LA UNIVERSIDAD DEL CAUCA.

En esta sección se presenta el diseño del sistema de alarmas de seguridad informática el cual buscó identificar los diferentes niveles de riesgo en los activos de información de la División de TIC de la Universidad del Cauca, y de manera eficiente, aplicar controles de seguridad que permitan el normal funcionamiento de los mismos.

Debido a lo anterior, se identificaron dos de los servicios con mayor nivel de riesgo en la División de TIC de la Universidad del Cauca, ya que sería demasiado extenso, para este trabajo de grado, realizar un análisis profundo para todos los servicios allí presentes.

2.3.1 Selección de dos (2) servicios críticos presentes en la División de TIC de la Universidad del Cauca.

La selección de los dos (2) servicios críticos se basó en la identificación, a través de las diferentes listas de chequeo y encuestas realizadas a los administradores, de las necesidades y requerimientos seguridad presentes en la División de TIC de la Universidad del Cauca.

Se pudo concluir que los servicios críticos a ser tratados son el WEB y el CORREO ELECTRONICO, superando a otros servicios como SIMCA. Esto se debió al análisis de vulnerabilidades y amenazas latentes sobre estos, además que se debe tener en cuenta la importancia jerárquica de los servicios y como estos dan pie para el funcionamiento de otros. Es el caso especifico del servicio WEB, que se considera un servicio principal y soporta otros servicios que podrían considerarse importantes como SIMCA.

Se podría suponer según la lista de chequeo realizada para identificación de servicios que los servicios sugeridos para ser tratados deberían ser el DNS y el PROXY, ya que estos son una posible puerta de entrada para atacantes o personas no autorizadas, pero se descartaron por el simple hecho de que para estos servicios se han ido implementando y aplicando, durante el desarrollo de este trabajo de grado, diferentes controles de seguridad por parte de los administradores de los servicios de la División de TIC’s de la Universidad del Cauca. Pero en cuanto a los servicios WEB y CORREO ELECTRONICO se encontró que no se han realizado aplicaciones seguras, y teniendo en cuenta su importancia y la integridad, disponibilidad y confidencialidad que deben prestar, es necesario tratarlos de manera urgente.

Se presenta una extracción como evidencia en la figura 8 de la evaluación realizada mediante la lista de chequeo para la identificación de los servicios críticos de la División de TIC de la Universidad del Cauca en donde se observa la importancia del servicio WEB:

	Servicios con los que cuenta la División de las TIC's	SI	NO	Observaciones
4.5	¿Si el servidor DNS falla, afecta a otros servicios? ¿Cuáles?	✓		*Todos los servicios WEB, navegación.*
4.6	¿Depende SIMCA que otros servicios estén funcionando? ¿Cuáles?	✓		*WEB, autenticación, base de datos.*
4.7	¿Se podría decir que el servicio más importante es el de WEB de la página Institucional?	✓		*Dado que es la cara visible a internet, es la puerta de entrada a otros servicios (WEB, correo), pero sin DNS no hay servicio WEB.*
4.8	¿Es aceptable la afirmación de que el servidor FTP, Correo, Proxy y WEB trabajan de modo independiente?	✓		*Trabajan independiente pero dependen del DNS para funcionar.*

Figura 8. Evidencia lista de chequeo de servicios críticos.

.

De igual manera a través de la encuesta realizada al administrador se da por entendido que estos servicios son también vitales para la división, por lo que esto hace parte de la probabilidad de impacto sobre un activo de información que se aplica en el instrumento de medición.

2.3.2 Herramientas de monitoreo para los servicios críticos de la División de TIC de la Universidad del Cauca.

En esta parte se planeó la integración del sistema de monitoreo Nagios, ya antes mencionado, con el sistema de alarmas de seguridad informática. Como ya se mencionó, Nagios hace parte fundamental del éxito del sistema, ya que es a través de él que el sistema de alarmas de seguridad informática realiza una consulta de estado de los servicios monitoreados. Este es un dato altamente confiable ya que sumado al resultado de la encuesta realizada a los administradores de los servicios, brinda un resultado de alta credibilidad de la probabilidad de que un activo de información sea afectado por una o varias amenazas.

2.3.3 Bases de datos

MySQL[18] es el sistema de administración de bases de datos utilizado en el sistema de alarmas de seguridad informática del presente proyecto de grado por presentar las siguientes características:

- Gestión de usuarios y contraseñas, manteniendo un muy buen nivel de seguridad en los datos.
- Condición de código abierto (open source) de MySQL, lo que hace que la utilización sea gratuita y se puede modificar con total libertad.
- Aprovecha la potencia de sistemas multiprocesador, gracias a su implementación multi-hilo.
- Dispone de API's[20] en gran cantidad de lenguajes como C, C++, Java, PHP, entre otros.
- Se puede descargar su código fuente. Esto ha favorecido muy positivamente en su desarrollo y continuas actualizaciones.
- Gran rapidez y facilidad de uso.
- Infinidad de librerías y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación.

La relación de las tablas utilizada para este proyecto de grado se especifica en las figuras 9, 10, 11, 12 y 13:

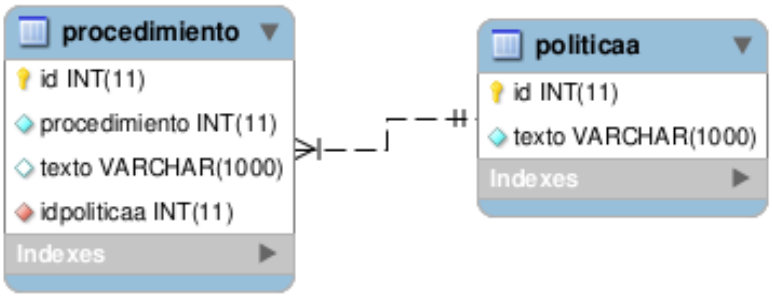


Figura 9. Relación de procedimientos.

[20] La Interfaz de programación de aplicaciones o API es un conjunto de funciones y procedimientos que puede ofrecer cierta biblioteca para en conjunto con otro software, ser utilizado como una abstracción.

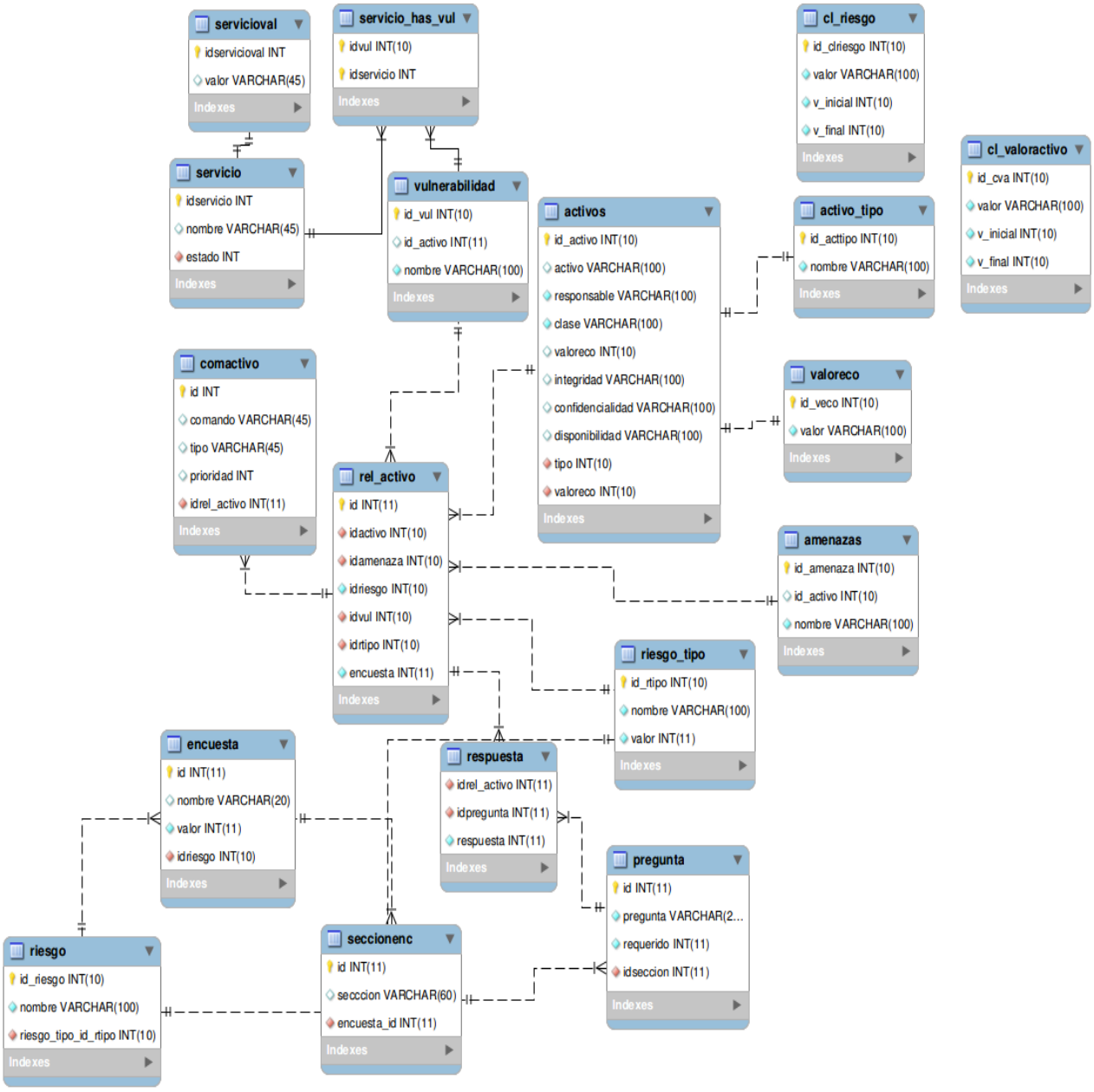


Figura 10. Relación extendida.

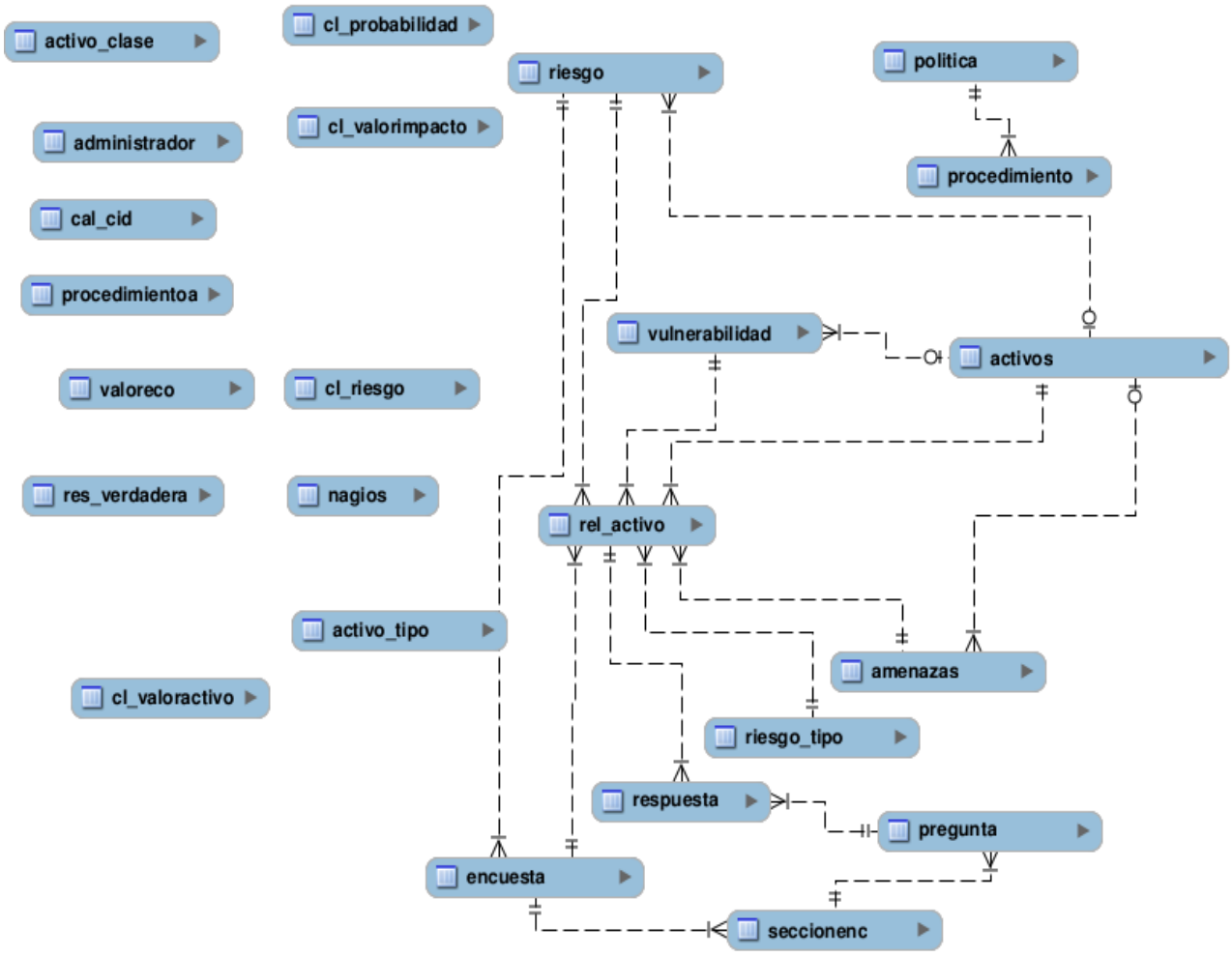


Figura 11. Relación general.

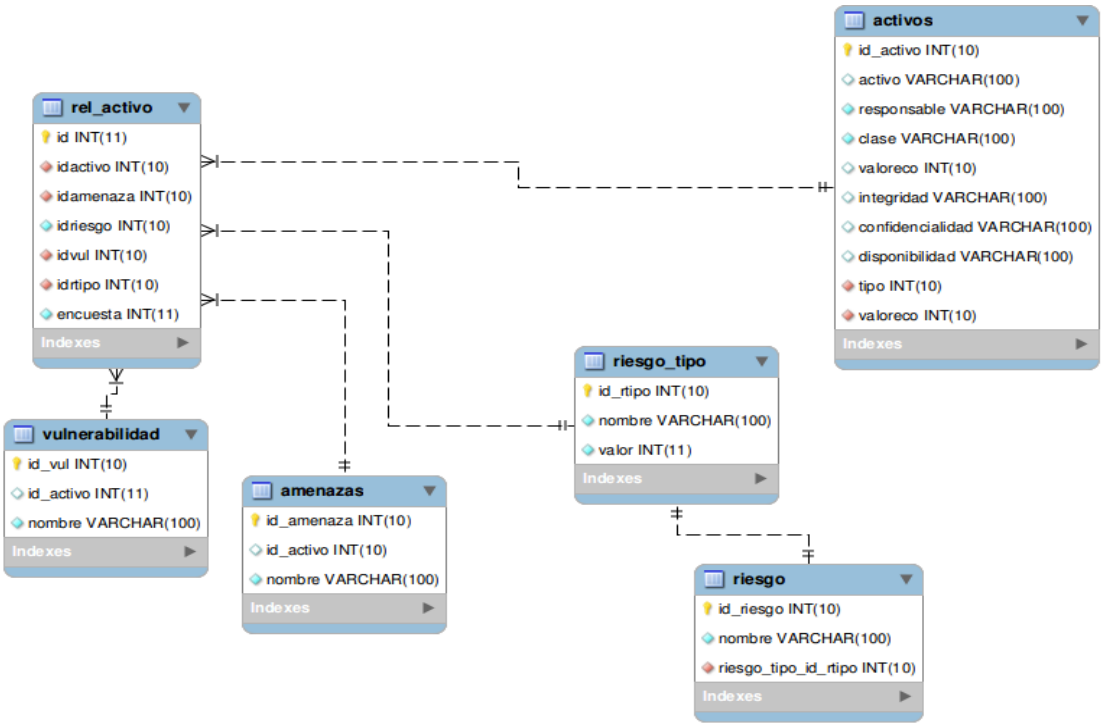


Figura 12. Relación riesgo.

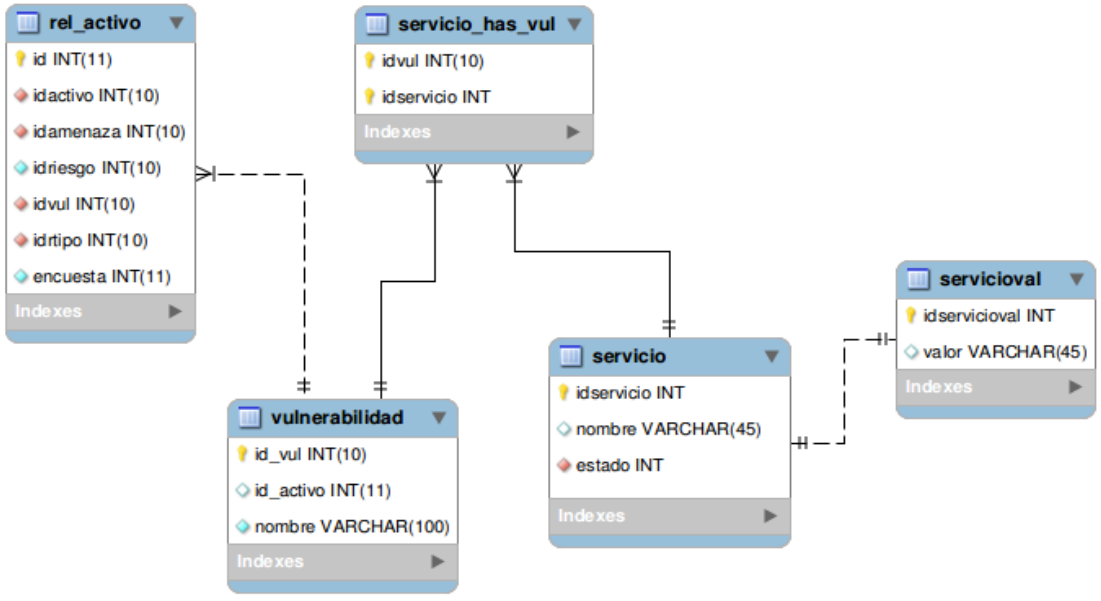


Figura 13. Relación Nagios.

2.3.4 PHP y JavaScript

El sistema de alarmas de seguridad informática para los servicios críticos de la División de TIC de la Universidad del Cauca utiliza, para el manejo de interfaz web, el lenguaje interpretador de alto nivel PHP (Hipertext Pre-processor) [19], el cual está embebido en páginas HTML [20]. Este es orientado al desarrollo de aplicaciones web dinámicas con las siguientes características:

- Capacidad de realizar conexión con la mayoría de los motores de bases de datos utilizadas (MySQL y PostgreSQL [21])
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite aplicar técnicas de programación orientada a objetos.
- No requiere definición de tipos de variables aunque sus variables se pueden evaluar también por el tipo que estén manejando en tiempo de ejecución.
- Tiene manejo de excepciones (desde PHP5[21]).
- Posee una amplia documentación en su sitio web oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.

JavaScript [22] es el lenguaje de programación utilizado para realizar la actualización de los datos que son consultados en la base de datos del sistema de alarmas de seguridad informática y tiene como tarea informar en pantalla el aumento del nivel de riesgo en los servicios críticos de la División de TIC de la Universidad del Cauca. Las principales características para el uso de este lenguaje son:

- Lenguaje basado en acciones que posee menos restricciones.
- Lenguaje de scripting[22] que es seguro y fiable.
- Permite la programación orientada a objetos.
- Su sintaxis es similar a la usada en Java y C. Al ser un lenguaje del lado del cliente, este es interpretado por el navegador por lo que no se necesita tener instalado ningún Framework[23].
- Compatible con varios tipos de navegadores como Internet Explorer, Netscape, Opera, Mozilla Firefox, entre otros.

[21] PHP5 es la última versión realizada por los desarrolladores de PHP. Para más información sobre esta versión visitar el siguiente enlace: http://administraciondesistemas.pbworks.com/f/Manual_PHP5_Basico.pdf
[22] Significa que se basa en la aplicación de scripts ya sea de manera local o remota.
[23] El famework o infraestructura digital es aquella que representa una arquitectura para la implementación o desarrollo de una aplicación.

2.3.5 Políticas de seguridad para dos (2) de los servicios críticos de División de TIC de la Universidad del Cauca.

Las políticas de seguridad y sus procedimientos son uno de los grandes pasos para desarrollar el SGSI. Se busca a través de ellas brindar una normatización segura para los procesos de una empresa, es por eso, que deben estar bien documentadas y al mismo tiempo, aplicadas según las necesidades de quien las implementa. Se debe resaltar que su integridad no se puede ver afectada, ya que un fallo en esto significa un sinnúmero de inconvenientes que pueden afectar los activos más valiosos de información.

En el desarrollo de este proyecto se utilizaron las políticas y procedimientos de seguridad de la información para el servicio CORREO ELECTRONICO, desarrollado por el grupo de investigación SGSI Unicauca en el cual participa el Ingeniero Siler Amador Donado, director del presente proyecto de grado. Este documento tiene por nombre: “Políticas de seguridad de los activos o recursos institucionales”[23], y fue realizado en el mes de agosto del año 2011 e integrado al presente proyecto de grado con el fin de realizar la aplicación de dichas políticas.

Se omite la explicación de estas políticas y procedimientos ya que no fue un desarrollo estrictamente de este proyecto y se remite al lector su consulta en la sección de anexos. Se puede ubicar en el Anexo B.1.

2.4 DESARROLLO DE UN SISTEMA DE ALARMAS DE SEGURIDAD INFORMÁTICA PARA DOS (2) DE LOS SERVICIOS CRÍTICOS DE RIESGO DE LA INFORMACIÓN PRESENTES EN LA DIVISIÓN DE TIC DE LA UNIVERSIDAD DEL CAUCA.

Una vez diseñado el sistema de alarmas de seguridad informática, se procedió a su desarrollo, integrando en su totalidad los componentes necesarios para poder brindar un análisis y gestión del riesgo, confiable, eficiente y eficaz del riesgo presente en la División de TIC de la Universidad del Cauca.

2.4.1 Monitoreo a través de Nagios para la generación de alarmas de los servicios y modificación del valor de riesgo.

El sistema de alarmas de seguridad informáticas actualiza cada 30 segundos los datos de los activos de información con sus respectivas vulnerabilidades, amenazas y valor de riesgo con el fin único de alarmar ante el aumento de nivel de riesgo y aplicar los respectivos controles.

Los datos son consultados en el sistema de monitoreo Nagios el cual está exportando en tiempo real los valores de los estados de los servicios adicionados mediante el plugin NDOUtils [24] (Nagios Data Out), siendo un add-on24 oficial de Nagios que permite exportar todos los sucesos y la configuración de una o más instancias de Nagios a una base de datos MySQL.

Al consultar el estado real de los activos de información, se actualiza en el sistema de alarmas de seguridad informática el valor de la probabilidad de ocurrencia con el fin de conocer el valor de riesgo según el análisis de riesgos utilizado en el presente proyecto de grado.

La información del incorrecto funcionamiento de alguno de los activos de información monitoreados es enviada por correo electrónico al responsable del servicio a través de la clase *phpmailer*[25] donde se configura el destinatario y el mensaje, en este caso la alarma a mostrar.

En el momento de existir un cambio en el estado de algún activo de información, se modifica el valor de riesgo y se despliega una alarma en pantalla informando la vulnerabilidad que ha sido atacada, para finalmente realizar la aplicación de los controles necesarios para llevar de nuevo el valor de riesgo a los parámetros aceptables en la organización.

Lo anterior se resume en la figura 14:

[24] Extensión, complemento o en este caso particular un plugin.
[25] http://blog.unijimpe.net/introduccion-a-phpmailer/

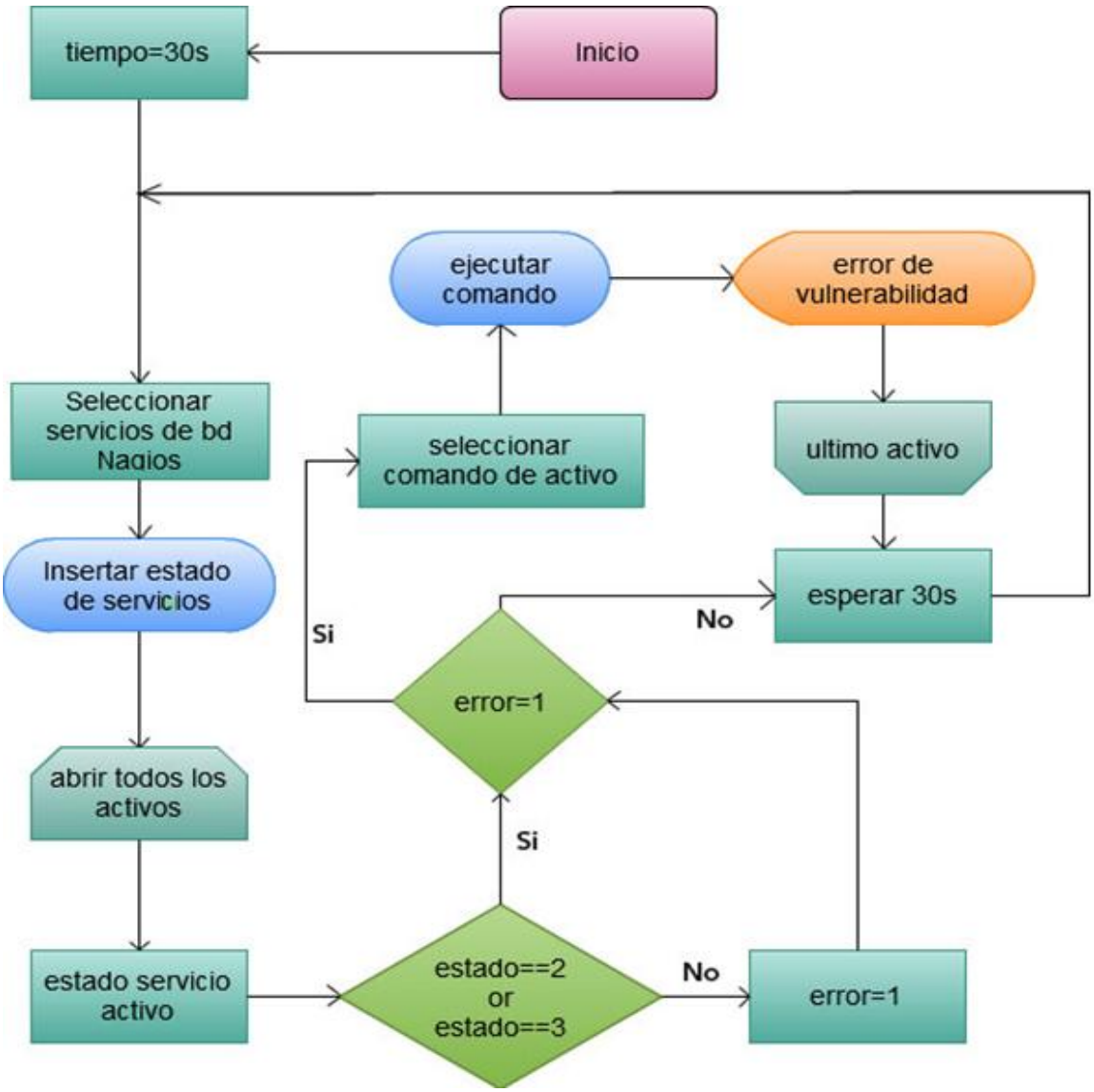


Figura 14. Diagrama de flujo del sistema de alarmas de seguridad informática.

El esquema general del sistema de alarmas de seguridad informática, que tiene por acrónimo *SASI*, se resume en la figura 15:

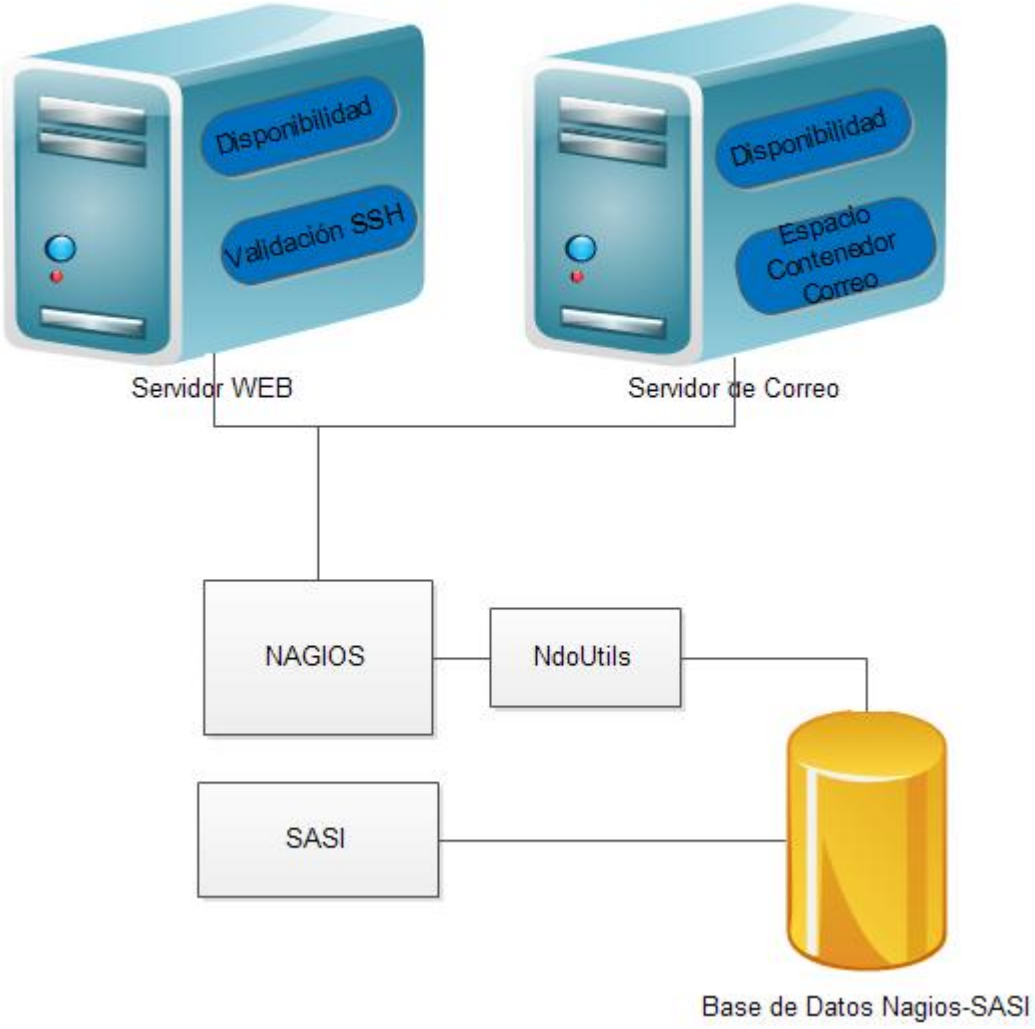


Figura 15. Estructura general del SASI.

2.4.2 Aplicación de controles ante el aumento considerable del valor de riesgo en los servicios seleccionados.

Se listan los diferentes controles que sirven para poder mitigar el valor de riesgo encontrado en los activos de información de la División de TIC de la Universidad del Cauca. Los controles se muestran en la tabla 13:

Control	Descripción
Control 1	Disponibilidad del servicio WEB
Control 2	Disponibilidad del servicio de CORREO ELECTRONICO
Control 3	Controlar las conexiones a los servidores por protocolo SSH[26] solo para usuarios autorizados
Control 4	Controlar la disponibilidad de espacio en disco duro donde se alojan los correos de la Institución
Control 5	Controlar el número de peticiones al servidor WEB para evitar una DoS.
Control 6	Controlar ataques por diccionario o fuerza bruta.

Tabla 13. Controles.

De los controles mencionados en la tabla anterior se procedió al diseño y desarrollo de cuatro (4) de ellos, pero por cuestiones temporales, se implementaron tres (3) de ellos, los cuales se integraron satisfactoriamente con el sistema de alarmas de seguridad informática para dos (2) de los servicios críticos de la Universidad del Cauca.

Los controles fueron implementados en el servidor local y se programó su ejecución cada periodo de tiempo haciendo uso del programador de tareas propio de Linux: Crontab [23].

Los tiempos de ejecución han sido establecidos de la siguiente manera:

- Control 1: Se ejecuta con frecuencia de 2 minutos.
- Control 2: Se ejecuta con frecuencia de 2 minutos
- Control 3: Se ejecuta con frecuencia de 1 minutos.

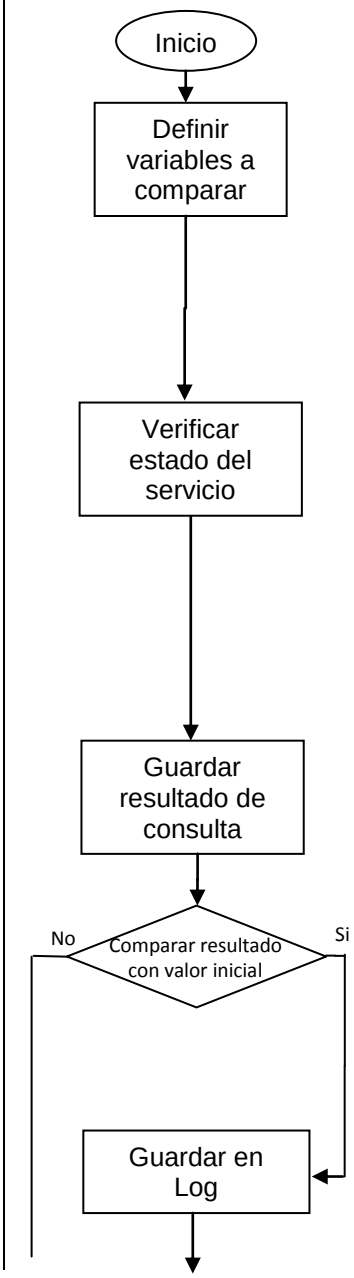
Los tiempos utilizados para la verificación y aplicación de los controles están ligados a los requerimientos de confidencialidad, disponibilidad e integridad de los activos de información.

Los controles diseñados para el sistema de alarmas informáticas fueron:

- **Control 1 y Control 2: verificación de disponibilidad de los servicios WEB y CORREO ELECTRONICO.** El funcionamiento de los controles para verificación del estado del servicio, ya sea WEB o CORREO ELECTRONICO, tienen una estructura similar, donde solo varía el log[27] que se revisa de cada servicio.

[26] Secure Shell o interprete de ordenes seguras es un protocolo utilizado para acceder a maquinas remotas de manera segura.

[27] Un log es un registro oficial de eventos durante un rango de tiempo. En el caso de la seguridad informática, es usado para registrar datos sobre cuando ocurre un evento en particular en una aplicación o dispositivo.

TAREA	RESPONSABLE	ACTIVIDAD
		
	Administrador del Servicio	Se definen las variables que serán comparadas para verificar el estado del servicio (WEB=0 o CORREO ELECTRONICO=0; siendo cero (0) el valor de servicio apagado)
	Administrador del Servicio	Existen dos forma de verificar el estado del servicio: a. Mediante los comandos correctos, se verifica el valor del estado del servicio específico. (0 = Servicio apagado y 1 = Servicio corriendo). b. Utilizando los resultados guardados en la base de datos del sistema de monitoreo Nagios.
	Administrador del Servicio	Se guarda el resultado de la consulta del estado del servicio específico (WEB o CORREO ELECTRONICO).
	Administrador del Servicio	Se guarda en un nuevo log denominado: iniciar_servicio.log el proceso de arranque del servicio.

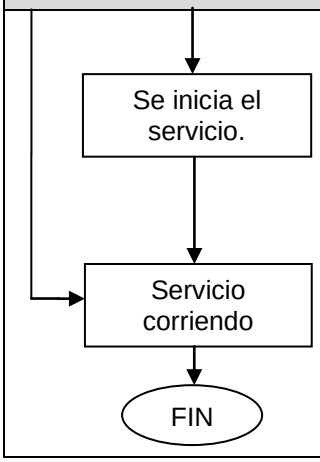
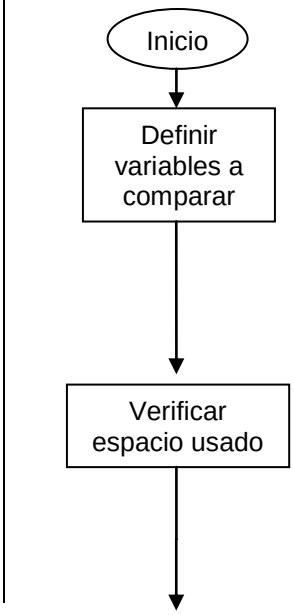
TAREA	RESPONSABLE	ACTIVIDAD
	Administrador del Servicio	Se ejecuta el comando correcto y el servicio que se desea iniciar. (WEB o CORREO ELECTRONICO)
	Administrador del Servicio	Se informa en pantalla que el servicio está en ejecución.

Figura 16. Flujograma del control de verificación de disponibilidad de los servicios.

- **Control 3: verificación del espacio libre en el disco duro del servidor de CORREO ELECTRONICO.** El control numero 3 verifica el espacio libre en el disco duro donde se encuentra el contenedor de las cuentas de correo electrónico de la Universidad del Cauca.

  El diseño se explica en la figura 17:

TAREA	RESPONSABLE	ACTIVIDAD
		
	Administrador del Servicio	Se definen las variables que serán comparadas para verificar el espacio libre en el disco duro. 80%-100% espacio usado = Crítico 40%-79% espacio usado = Normal 0%-39% espacio usado = Disco Libre
	Administrador del Servicio	Existen dos forma de verificar el estado del servicio: a. Mediante los comandos correctos, se verifica el espacio usado por las cuentas de correo electrónico en el disco duro. b. Utilizando los resultados guardados en la base de datos del sistema de monitoreo Nagios.

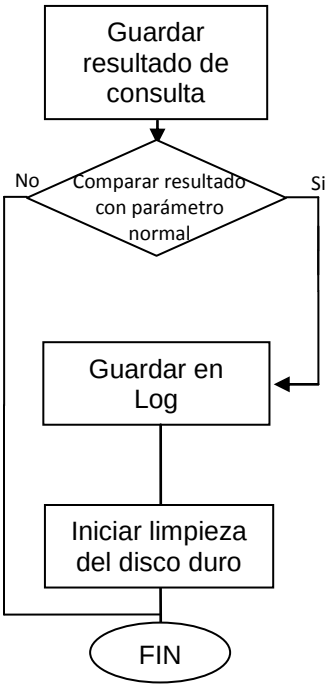
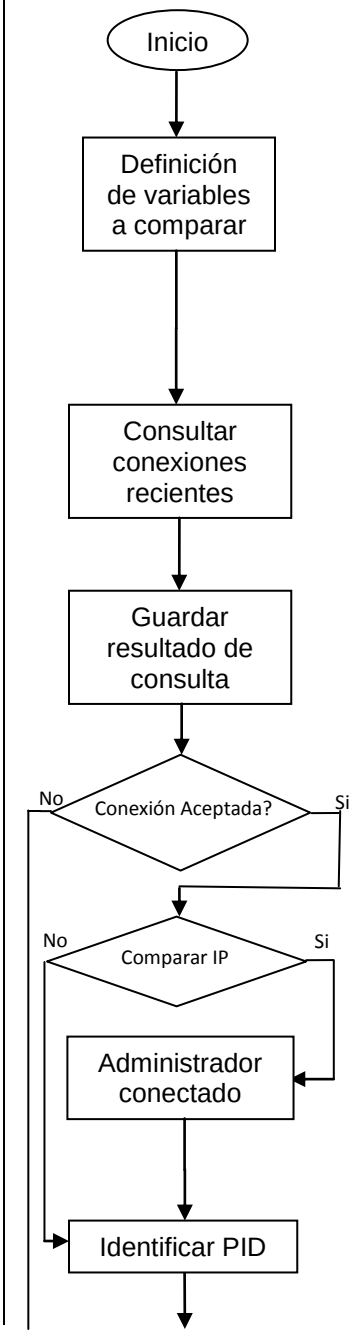
TAREA	RESPONSABLE	ACTIVIDAD
	Administrador del Servicio	Se guarda el resultado de la consulta del estado del servicio específico, bien sea por comandos en la shell[28] o por consulta a base de datos de Nagios.
	Administrador del Servicio	Se guarda en un nuevo log denominado “disco_libre.log” el proceso de limpieza del disco.
	Administrador del Servicio	Se inicia la depuración de la información del disco duro según las políticas establecidas por la Universidad del Cauca.

Figura 17. Flujograma del control de verificación de espacio libre en el disco duro del servidor de CORREO ELECTRONICO.

- **Control 4: Monitoreo de las conexiones por SSH al servidor WEB.** Es necesario controlar las conexiones realizadas al servidor WEB de la Universidad del Cauca con el fin de disminuir el riesgo de modificación, pérdida o robo de información.

  El funcionamiento del presente control está explicado en la figura 18:

[28] Interfaz de usuario de línea de comandos.

TAREA	RESPONSABLE	ACTIVIDAD
		
	Administrador del Servicio	Se definen variables estáticas que serán comparadas con los datos obtenidos tras la conexión por parte de cualquier usuario. La primera variable almacena si hay conexiones exitosas y la segunda variable almacena la dirección IP que usa el responsable para la administración del servicio.
	Administrador del Servicio	Mediante consola se consulta el log donde se almacenan las conexiones recientes por SSH al servidor WEB.
	Administrador del Servicio	Se guarda el resultado de la consulta de las conexiones recientes para luego ser comparadas con las variables fijas.
	Administrador del Servicio	Se guarda en un nuevo log denominado “admin_valido.log” y se confirma que es el administrador.
	Administrador del Servicio	Se identifica el PID[29] del proceso de conexión SSH.

[29] Process ID o Identificador de procesos. El identificador de procesos es un número entero usado por el kernel de algunos sistemas operativos para identificar un proceso de forma unívoca.

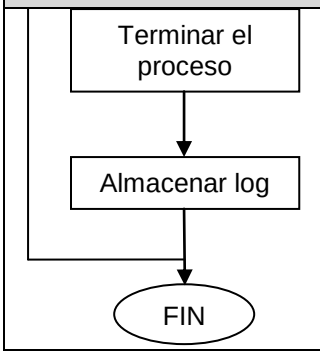
TAREA	RESPONSABLE	ACTIVIDAD
	Administrador del Servicio	Se termina el proceso con el PID identificado.
	Administrador del Servicio	Se guarda en un archivo la ejecución del control para medir la eficiencia del mismo.

Figura 18. Flujograma del control de monitoreo de conexiones por SSH al servidor WEB.

2.4.3 Proceso de gestión de riesgo e interfaz final del sistema de alarmas de seguridad informática.

En la figura 19 se muestra el diagrama de flujo de los diferentes procesos de gestión del riesgo realizado por el sistema de alarmas de seguridad informática para dos (2) de los servicios críticos de la División de TIC de la Universidad del Cauca:

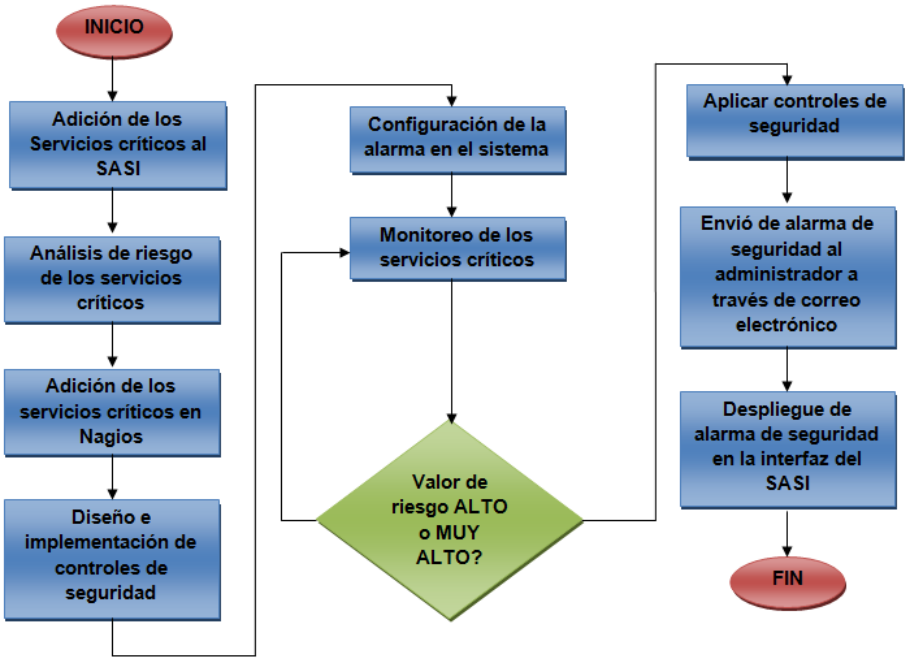


Figura 19. Diagrama de flujo de los procesos de gestión del SASI.

Finalmente se presentan en las figuras 20, 21, 22, 23 y 24 las evidencias respectivas de la interfaz del sistema de alarmas de seguridad informática, donde se visualizan diferentes procesos como: adición de activos de información, políticas de seguridad, encuesta al administrador de los servicios, entre otros.

Figura 20. Interfaz de inicio del SASI.

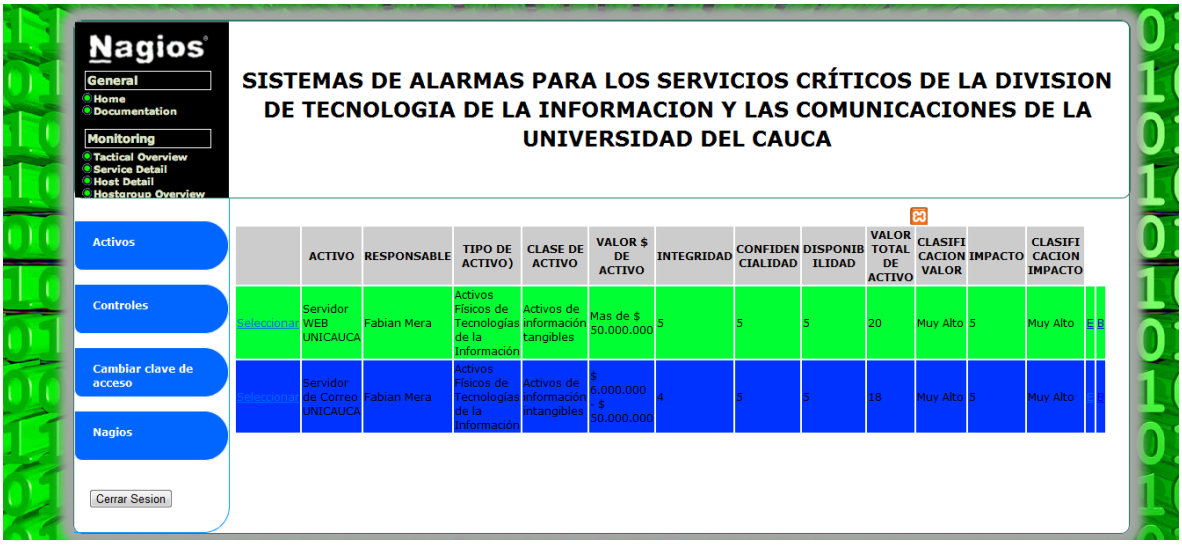


Figura 21. Interfaz de activos de información y valores de riesgo del SASI.

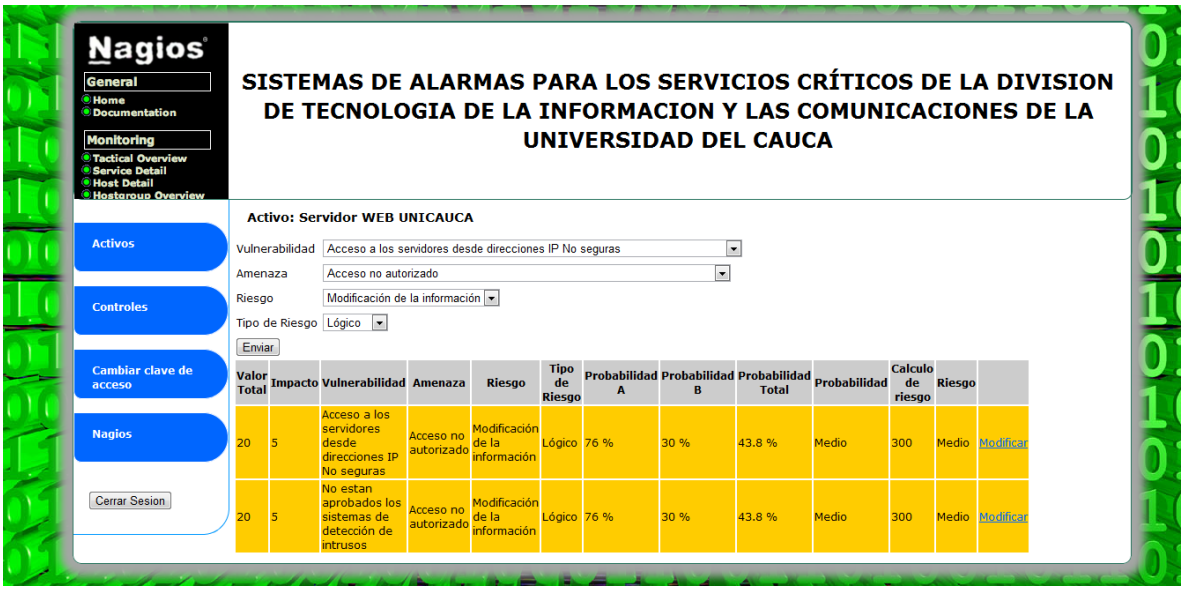


Figura 22. Interfaz de vulnerabilidades, amenazas y riesgos para cada activo de información del SASI.

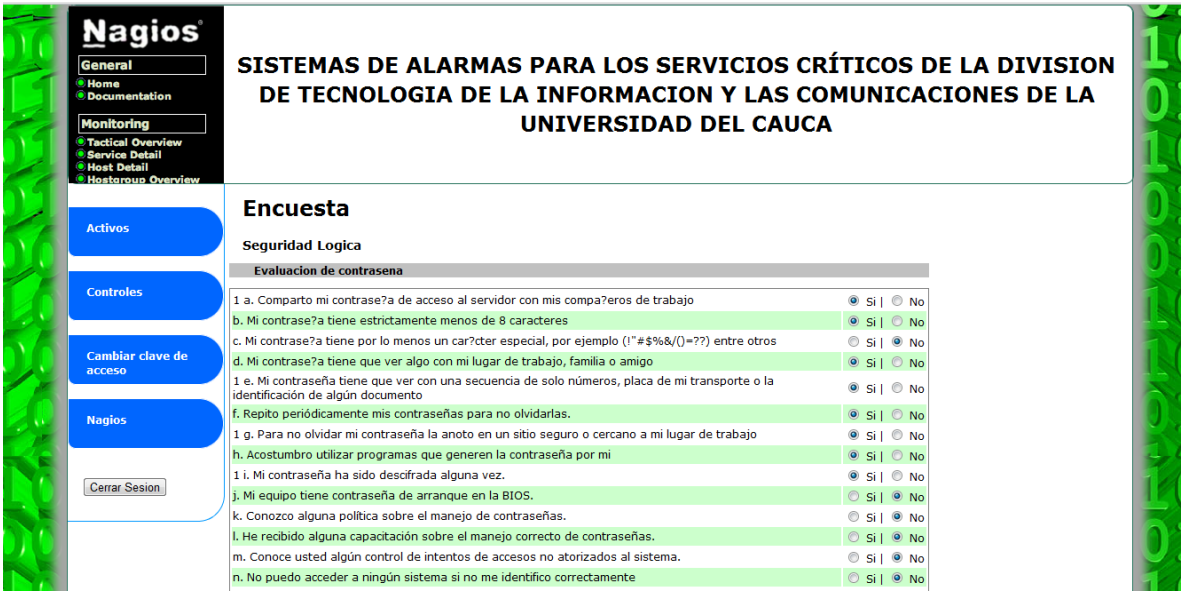


Figura 23. Interfaz de encuesta al administrador del activo de información del SASI.

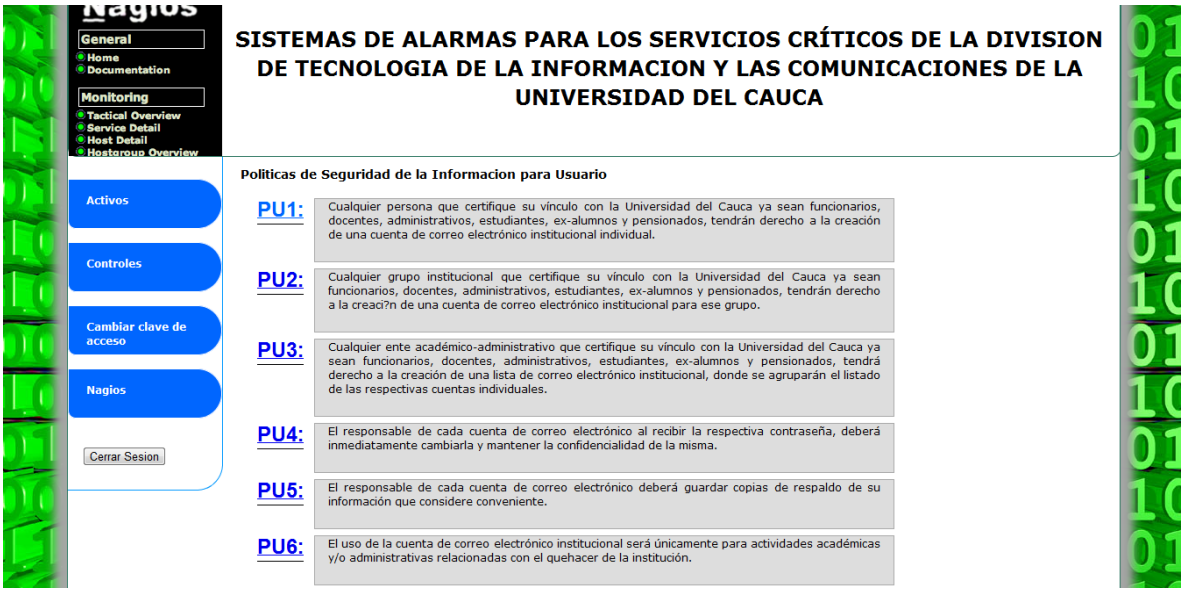


Figura 24. Políticas de seguridad del SASI.

3. ANÁLISIS DE RESULTADOS.

En esta sección se realiza un análisis del comportamiento de la herramienta desarrollada, tanto la medición de los niveles de riesgo como su comportamiento ante una amenaza, y por ende, la aplicación de uno o más controles necesarios para mitigar el valor de riesgo.

3.1 DESARROLLO DE PRUEBAS NECESARIAS PARA MEDIR EL FUNCIONAMIENTO DEL SISTEMA DE ALARMAS DE SEGURIDAD INFORMÁTICA.

Las pruebas realizadas al sistema de alarmas de seguridad informática de la División de TIC se centraron en un entorno virtual de los activos de información de la Universidad del Cauca. El responsable de los servicios de información, tales como el servicio WEB y el CORREO ELECTRONICO, facilitó una réplica instalada en máquinas virtuales con acceso VPN para poder realizar las pruebas necesarias en cuanto a eficacia del sistema desarrollado.

Para lo anterior se hizo uso de las siguientes herramientas ya mencionadas:

- **Entorno virtual:** VMWare Workstation
- **Sistema operativo:** Linux Debian 5.0
- **Servidor web:** Apache 2.2.9
- **Servidor de correo:** Sendmail
- **Sistema de monitoreo:** Nagios
- **Base de datos:** MYSQL
- **Lenguaje de programación:** PHP

Los tiempos de respuesta de la aplicación quedaron establecidos de la siguiente manera:

1. El sistema de monitoreo Nagios verifica el estado de los activos de información con una frecuencia de 10 segundos.
2. El sistema de alarmas de seguridad informática realiza una actualización de los datos consultados en la base de datos del sistema de monitoreo Nagios cada 30 segundos.
3. Los controles implementados 1, 2, 3, de la tabla 13 se ejecutan según el nivel de disponibilidad, integridad y confidencialidad que requieran los activos de

información. En el presente proyecto los tiempos de ejecución quedaron establecidos según el numeral *2.4.2 Aplicación de controles ante el aumento considerable del valor de riesgo en los servicios seleccionados.*

Se realizó la simulación del sistema de alarmas de seguridad informática en dos escenarios, permitiendo efectuar diferentes amenazas sobres los servicios críticos seleccionados.

La figura 25 presenta el primer escenario donde se evaluó la disponibilidad de los servicios WEB y CORREO ELECTRONICO por parte del sistema de alarmas de seguridad informática.

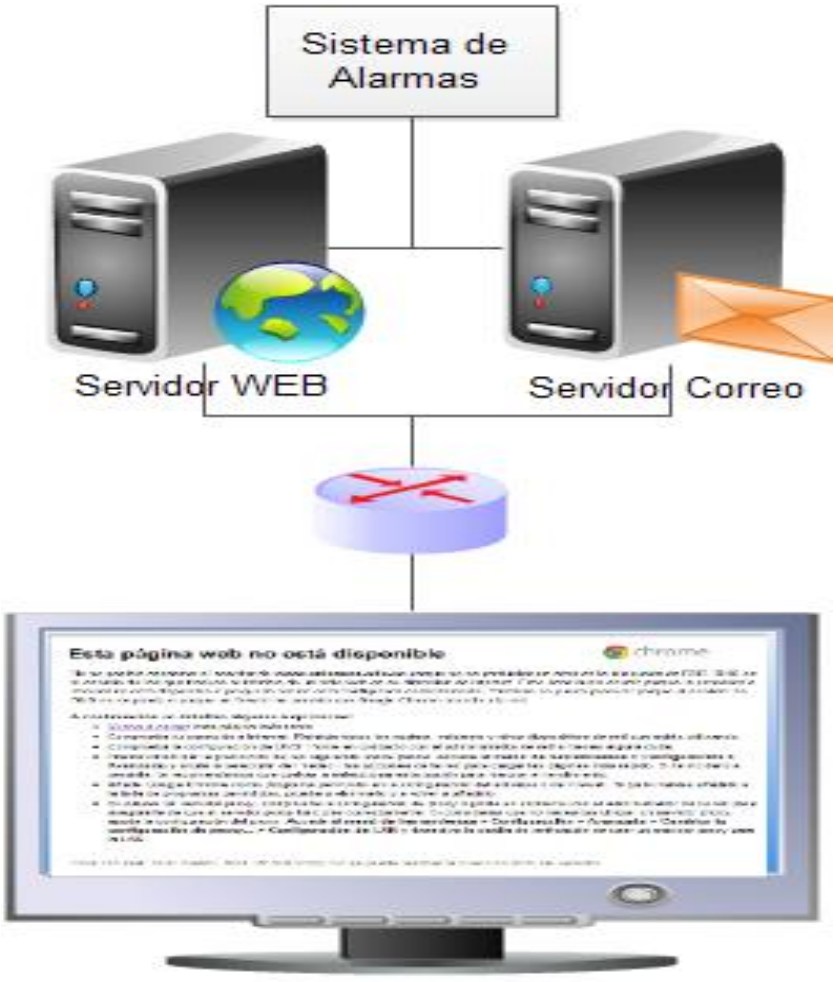


Figura 25. Primer escenario para desarrollo de pruebas del SASI.

La figura 26 presenta el segundo escenario de simulación el cual permitió desarrollar pruebas de una conexión no segura mediante protocolo SHH y que el sistema de alarmas de seguridad lo detectara y tomara decisiones.

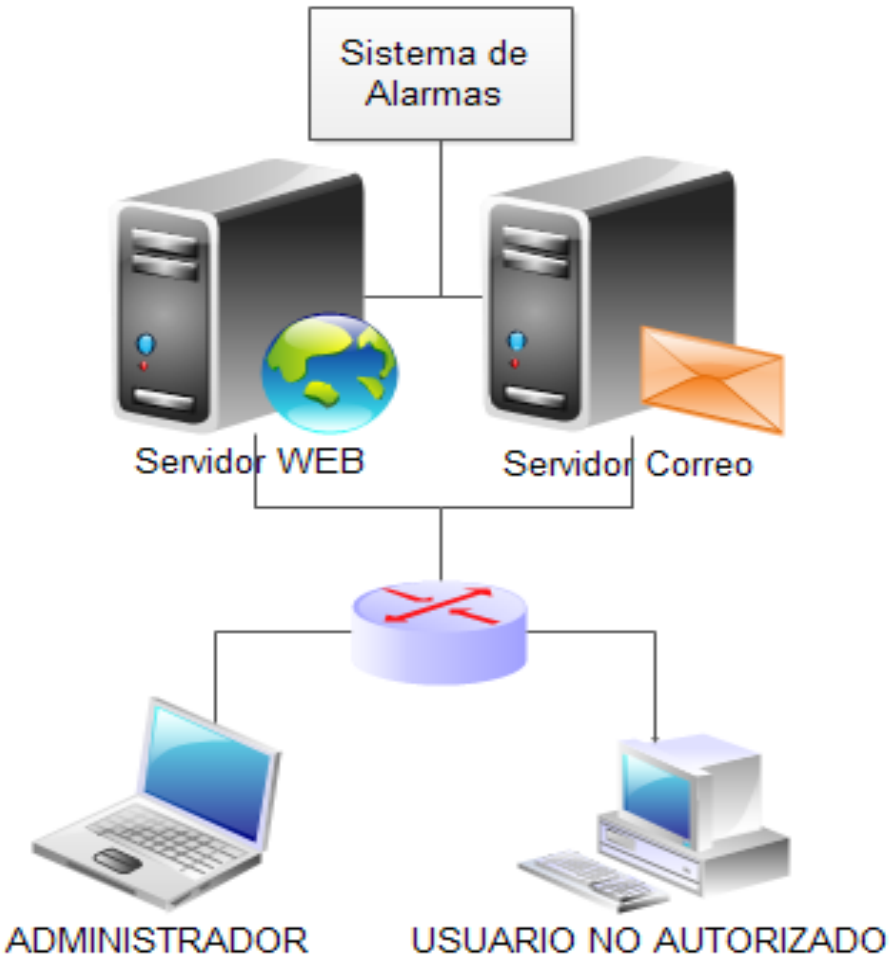


Figura 26. Segundo escenario para desarrollo de pruebas del SASI.

El tiempo de monitoreo, actualización de valor de riesgo y ejecución de los controles es el indicado para la visualización del funcionamiento del sistema de alarmas de seguridad informática por el responsable.

3.2 EVALUACIÓN DE LA EFICACIA DEL SISTEMA DE ALARMAS DE SEGURIDAD INFORMÁTICA.

Con el fin de medir la eficacia del sistema de alarmas de seguridad informática en los activos de información de la División de TIC de la Universidad del Cauca, se definieron dos (2) indicadores:

- **Indicador de disponibilidad de los servicios:** indica el porcentaje exitoso de ejecución del control de inicio de los servicios WEB y CORREO ELECTRONICO tras la caída o no disponibilidad de los mismos.

$$Inicio\ del\ servicio\ de\ correo\ = \frac{\#\ Ejecución\ exitosa\ del\ control}{\#\ \ Veces\ que\ el\ servicio\ de\ correo\ presento\ caida} * 100\%$$

El porcentaje obtenido en este indicador para el servicio WEB fue de un 92% de ejecución correcta del control. El 8 % restante corresponde al valor de porcentaje que el control no fue capaz de iniciar el servicio.

El porcentaje obtenido en este indicador para el servicio de CORREO ELECTRONICO fue del 85% de ejecución correcta del control. El 15% restante corresponde al valor de porcentaje que el control no fue capaz de iniciar el servicio por no encontrar cambios en el estado del mismo, esto se presenta por encontrar en dos (2) procesos el mismo nombre del servicio. Se puede visualizar las mediciones realizadas en la figura 27.

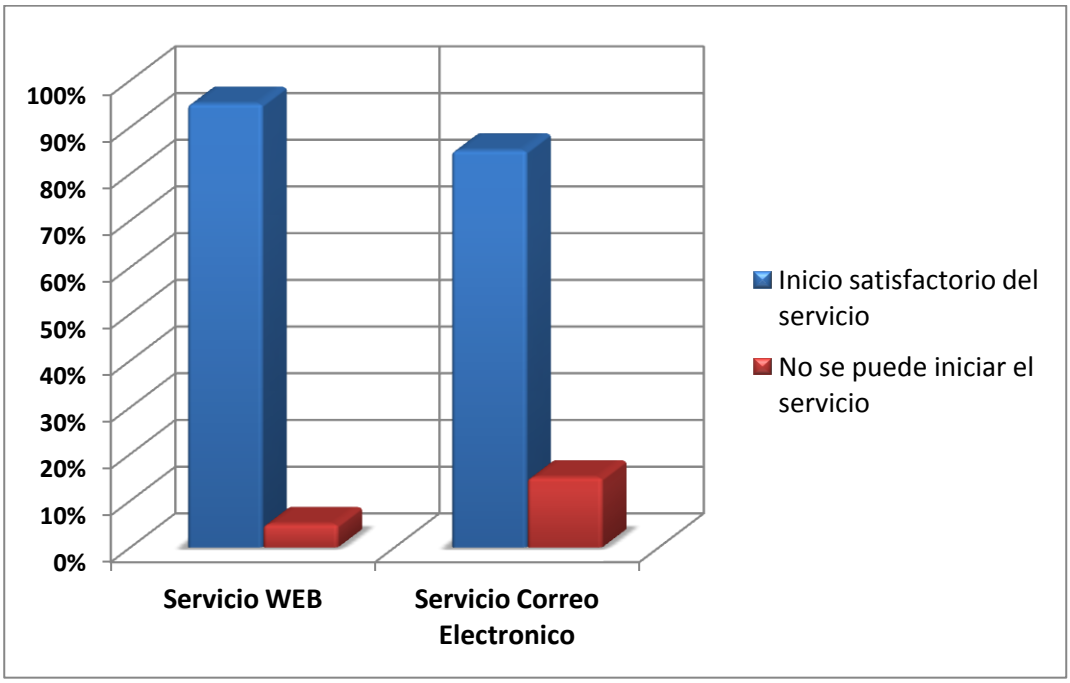


Figura 27. Indicador de disponibilidad de los servicios WEB y CORREO ELECTRONICO.

- **Indicador de conexiones bloqueadas**: indica el porcentaje de conexiones bloqueadas tras presentarse conexiones exitosas desde direcciones IP no registradas.

$$Conexión\ SSH\ = \frac{\#\ Conexiones\ bloqueadas}{\#\ \ Conexiones\ aceptadas\ desde\ direcciones\ IP\ no\ registradas} * 100\%$$

El resultado obtenido tras la implementación del control de conexión por SSH corresponde a un 95% de bloqueo correcto para la administración de los servicios. El 5% restante corresponde al porcentaje de que el sistema no fue capaz de detectar una conexión no autorizada por el constante cambio en el log, generando la necesidad de disminuir el tiempo de ejecución del script en el programador de tareas, logrando obtener resultados de bloqueo exitosos en la totalidad de conexiones no autorizadas. La figura 28 muestra los resultados obtenidos.

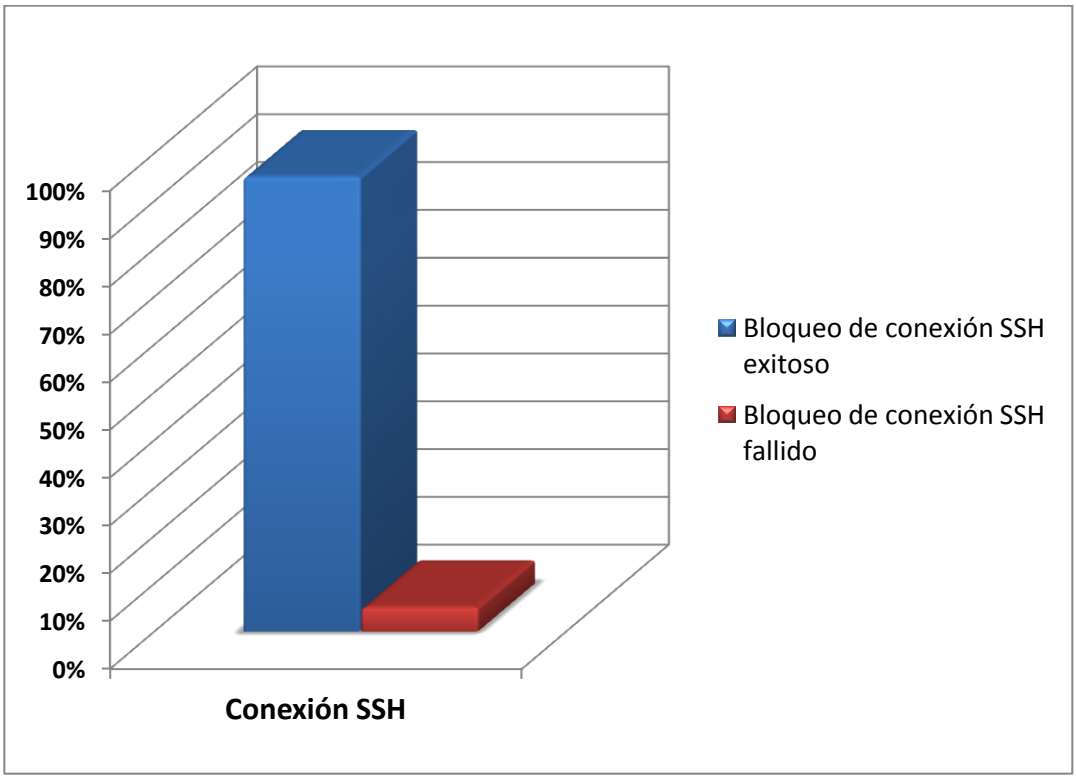


Figura 28. Indicador de bloqueo de conexiones SSH no autorizadas.

3.3 VENTAJAS OBTENIDAS A TRAVÉS DEL SISTEMA DE ALARMAS DE SEGURIDAD INFORMÁTICA.

Es importante detectar las ventajas que brinda el desarrollo de aplicaciones de gestión de riesgo en las empresas. Es por eso que se enuncian algunas de las ventajas del SASI:

- ✓ Análisis de riesgos de los activos de información seleccionados.
- ✓ Disponibilidad de los activos de información.
- ✓ Confidencialidad de los activos de información.
- ✓ Información completa de la materialización de las amenazas sobre las vulnerabilidades a los interesados.
- ✓ Estado de los activos de información en tiempo real.
- ✓ El sistema de alarmas de seguridad informática se adapta a cualquier organización independiente del tipo de negocio.

4. CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS.

En este capítulo final se presenta la conclusión del proyecto como también la identificación y sugerencia de mejoras en el denominado Sistema de alarmas de seguridad informática para los servicios críticos de la División de TIC de la Universidad del Cauca.

4.1 CONCLUSIONES.

Se presentan a continuación las conclusiones del presente proyecto basándose en los resultados obtenidos que dan por cumplido los objetivos generales y específicos propuestos para el desarrollo del mismo.

- La investigación determinó que la falta de sistemas de gestión de riesgos en el mercado que brinden un soporte estándar y compacto hacen que este proyecto sea un sistema novedoso e innovador, que mezcla la eficiencia de herramientas de monitoreo como Nagios y la aplicación de controles de seguridad como los propuestos en la norma ISO/IEC 27001:2005.
- El diseño y desarrollo de las fases de implantación de un Sistema de Gestión de Seguridad de la Información se basa en el ciclo PHVA, que permite al proyecto enfocarse correctamente en las necesidades de la División de TIC de la Universidad del Cauca. Estas fases aportan en la creación de lineamientos para la aplicación de un SGSI dentro de cualquier organización.
- El análisis y estudio de los activos de información de la Universidad del Cauca, en este caso los servicios con los que cuenta, permitió observar que a pesar de que se cuenta con ciertos niveles de seguridad dentro de la División de TIC, es aún insuficiente, ya que no se encuentran estandarizados por una norma nacional o internacional como la ISO/IEC 27001:2005 y esto da pie a generar inconsistencias dentro de la organización como brechas de seguridad que permiten a las amenazas explotar una o varias vulnerabilidades generando riesgos de seguridad de la información.
- El desarrollo de un instrumento de medición basado en el estándar ISO/IEC 27005:2008, permitió el análisis de riesgo de los servicios de información de la División de TIC de la Universidad del Cauca mostrando como resultado un nivel aceptable de seguridad implementado, además de la carencia de controles funcionales y automáticos como los implementados en este trabajo de grado que permiten solventar problemas en un tiempo aceptable.

- El análisis de riesgo utilizado en el sistema de alarmas de seguridad informática es confiable por obtener los valores deseados de los activos de información en tiempo real mediante el sistema de monitoreo Nagios.
- La medición a través de los indicadores mostro que la gestión del riesgo es efectiva en un alto grado de confianza, ya que la ejecución de los controles de seguridad permite a los servicios estar disponibles y mantener su confidencialidad en niveles óptimos.
- El sistema de alarmas de seguridad informática está concebido para ser implementado en cualquier organización independiente si es pública, privada, de servicios o de producción; por tener como base fundamental la norma ISO/IEC 27001:2005, además de dar cumplimiento a ciertos controles sugeridos en el anexo A de la norma mencionada.

4.2 RECOMENDACIONES

Se busca proponer una serie de recomendaciones que permita la evolución y mejora de la gestión de la seguridad de la información dentro de la División de TIC de la Universidad del Cauca.

- Es necesaria la certificación legal de la Universidad del Cauca por parte de organismos competentes en el estándar ISO/IEC 27001:2005, que permita contar con soporte eficaz y eficiente para brindar seguridad a los activos de información.
- Se recomienda dar uso a las fases desarrolladas en el apartado 2.1 de trabajo de grado para realizar un correcto desarrollo de un SGSI dentro de la División de TIC de la Universidad del Cauca lo cual permitirá una estructura organizada y funcional de gestión de la seguridad de los activos de información.
- Se debe contar con un mejor soporte documental dentro de la División de TIC de la Universidad del Cauca ya que los registros no son claros y muchos de ellos o casi todos no se encuentran desarrollados dentro de un marco estándar, por lo que esto puede generar inconvenientes técnicos y esto convertirse en pérdidas para la Universidad.

4.3 TRABAJOS FUTUROS

Ya que este proyecto es apenas la primera etapa de un macro proyecto de la implementación de un SGSI dentro de la Universidad del Cauca, se busca proponer una serie de pautas que permitan a los futuros desarrolladores de este proyecto tener referencias claras de las necesidades a implementar.

- Aunque el resultado fue el esperado en el instrumento de medición haciendo uso del estándar ISO/IEC 27005:2008, se puede recurrir a la posibilidad del desarrollo de un instrumento de medición de riesgo basado en normas como: NIST 800-30, GAO, OCTAVE, MAGERIT, IRAM, CORAS, entre otras, que permitan el desarrollo de un análisis mediante otra metodología para así comparar los resultados obtenidos y la efectividad de cada implementación.
- Se propone el desarrollo e implementación a futuro de los controles mencionados en la tabla 13 de este trabajo de grado, ya que esto significa brindar soporte y seguridad con un nivel alto de confianza a los servicios críticos seleccionados, como lo son el WEB y el CORREO ELECTRONICO.
- Se propone el análisis de riesgo para los servicios no tratados en este trabajo de grado como: SIMCA, DNS o PROXY, y así desarrollar políticas, procedimientos y controles que permitan disminuir los niveles de riesgo a un nivel aceptable por la Universidad del Cauca.
- Se propone el diseño e implementación del envió de la información en logs con el fin de tener indicadores de gestión de la eficiencia y eficacia de los controles, siendo un requisito importante en un Sistema de Gestión de la Seguridad de la Información.
- Integrar el sistema de alarmas de seguridad informática con los sistemas de control de acceso de la Universidad del Cauca para dar cumplimiento al objetivo de control “A.9.1 *Área Seguras”* del estándar ISO/IEC 27001:2005.
- Se propone el análisis y diseño de indicadores para medir la eficiencia por control en el sistema de alarmas de seguridad informática, para así obtener valores de tiempo de ejecución confiables tanto para la seguridad en la ejecución de los controles como para evitar fallos en los servicios críticos por carga de procesamiento o saturación de la memoria temporal.

5. BIBLIOGRAFÍA.

[1] ICONTEC. *"Estándar Internacional ISO/IEC 27001:2005 Information Technology -- Security techniques --Specification for an Information Security Management System"*. Disponible en: http://www.iso27001standard.com/es/iso-27001/blog

[2] ICONTEC. *"Estándar Internacional ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management"*. Disponible en: http://www.iso27001security.com/html/27005.html

[3] HACHIELO. *"El Ciclo PDCA (ciclo Deming)"*. Disponible en: http://ticss.bligoo.com/content/view/472119/Circulo-de-Deming.html

[4] SERRANO, Carlos. *"Modelo integral para el profesional en ingeniería"*. Disponible en: ftp://jano.ucauca.edu.co/proc_acred/Busqueda%20de%20la%20Excelencia/

[5] JOSKOWICZ, Jóse. *"Reglas y Prácticas en eXtremeProgramming"*. Disponible en: http://iie.fing.edu.uy/~josej/docs/XP%20-%20Jose%20Joskowicz.pdf

[6] INTECO. *"Sistema de Gestión de Seguridad de la información en una Organización"*. Available: http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/

[7] ISO27000, "Tratamiento de Riesgos,". Disponible en: http://www.iso27000.es/doc_sgsi_all_archivos/image002.gif

[8] ICONTEC. *"Controles ISO 27002:2005"*. Disponible en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

[9] ISO/IEC. *"Estandar Internacional ISO/IEC 17799"*. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[10] AVELLANEDA, Cao. "Análisis e impacto de riesgo". Disponible en: http://1.bp.blogspot.com/_ZyTVfswPHds/SE6MavoKi0I/AAAAAAAAAZI/uDlGmo-TUD8/s320/AGR.jpg

[11] ICONTEC. "Proceso de gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008". Disponible en: http://3.bp.blogspot.com/_8OViozpv-ps/SX7xUrdEVLI/AAAAAAAAAAk/o3TgMNroPEs/s400/Imagen1.png

[12] NAGIOS. *" Nagios"*. Disponible en: http://www.nagios.org/

[13] NAGIOS. "Estructura del sistema de monitoreo Nagios". Disponible en: http://nagios.sourceforge.net/download/contrib/documentation/misc/Nagios_spanish.pdf

[14] AWSTATTS. *"AWstats"*. Disponible en: http://awstats.sourceforge.net/

[15] SARG. *"SARG"*. Disponible en: http://sarg.sourceforge.net/

[16] FORTINET. *"FortiGate"*. Disponible en: http://www.fortinet.com/products/fortigate/

[17] Allot. *"NetXplorer"*. Disponible en: http://www.altimate.es/blobs/com.cardiweb.cardiboxv6.cm.business.Article/1707518580286817194/file/1/netxplorer_esp.pdf

[18] MYSQL. *"MySQL"*. Disponible en: http://www.mysql.com/

[19] JIMENEZ, Enri. *"PHP Avanzado"*. Disponible en: http://enrigimenez.com/wp-content/uploads/2008/03/php_avanzado.pdf

[20] FERRER, Jorge; GARCIA, Victor; GARCIA, Rodrigo. *"Curso Completo de HTML"*. Disponible en: http://es.tldp.org/Manuales-LuCAS/doc-curso-html/doc-curso-html.pdf

[21] POSTGRESQL. *"PostgreSQL"*. Disponible en: http://www.postgresql.org/

[22] RODRIGUEZ, Jose Antonio. *"Manual de JavaScript"*. Disponible en: http://cepa.elmolar.educa.madrid.org/temario-web/Javascript.pdf

[23] Grupo SGSI Unicauca. "Politicas de seguridad de los activos o grupos institucionales".

[24] GALSTAD, Ethan. *"NDOUTILS Documentation Version 1.4"*. Disponible en: http://nagios.sourceforge.net/docs/ndoutils/NDOUtils.pdf

[25] Ajaxman. *"Crontab"*. Disponible en: http://www.intitec.com/varios/crontab.pdf