CRITERIOS PARA ESTABLECER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PLAN DE CONTINGENCIA, CASO DE ESTUDIO EL CENTRO DE DATOS DE LA UNIVERSIDAD DEL CAUCA

Anexos

Carolina Guevara Campo
Fabián Andrés Mera

Director: Ing. Siler Amador Donado.
Codirector: Ing. Jaime Andrés Gaviria Molano

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas

Popayán, Marzo de 2008

Tabla de contenido

Tabla de contenido 2
Lista de figuras 4
Lista de Tablas 5
1 Generalidades de las normas para la seguridad de la información 7
1.1 Normas para la seguridad de la información 7
1.1.1 Normas ISO 27000 7
1.2 Norma ISO 27001 7
1.2.1 Compatibilidad con otros sistemas de gestión 9
1.2.2 Sistema de Gestión de Seguridad de la Información 10
1.2.3 Anexos ISO 27001 10
1.3 ISO 17799 11
1.3.1 Los controles de ISO 17799 11
1.4 Normas complementarias para seguridad de la información 12
1.4.1 ISO 13335 12
1.4.2 ISO 15408 12
1.4.3 ISO 21827 12
1.4.4 BS 7799 12
1.4.5 FISMA Proyecto estadounidense 13
1.4.6 FIPS 140-2 Ley Estadounidense 14
1.4.7 Ley Sarbanes-oxley 15
1.4.8 COBIT 16
1.4.9 RFC 2196 17
1.4.10 Manual de protección para tecnologías de la información 17
1.4.11 OECD 17
1.4.12 ISO 15408 18
1.4.13 Serie arco iris Rainbow Series (orange books) (EE.UU) 18
1.4.14 ITSEC Reino Unido 18
1.4.15 CMM 19
1.4.16 SSE-CMM 19
1.4.17 ISO 11131 19
1.4.18 ISO 13569 20
2 Anexo análisis de riesgos 21
2.1 Introducción 21
2.2 Definición de análisis de riesgos 21
2.2.1 Limitaciones de la gestión del riesgo 24
2.2.2 Estrategias para la gestión del riesgo 24
2.2.3 Importancia de la gestión del riesgo 24
2.3 Metodologías para el análisis de riesgos 25
2.3.1 SOMAP 25
2.3.2 Magerit 26
2.4 Herramientas para el análisis y gestión de riesgos 28
2.5 Aplicación de una metodología de análisis de riesgos en una institución educativa 31
2.5.1 Fases del desarrollo 31
2.5.2 Activos 33
2.5.3 Determinación de las amenazas 37
2.5.4 Determinación del impacto 38
2.5.5 Determinación de un riesgo 38

2.5.6 Determinación de medidas de protección 39
2.5.7 Documentación a entregar para el análisis de riesgos 40
2.6 Análisis inicial para recolección de información 41
2.6.1 Alcance 41
2.6.2 Políticas de seguridad de la información 41
2.6.3 Organización de la seguridad 42
2.6.4 Control y clasificación de activos 42
2.6.5 Seguridad del personal 42
2.6.6 Seguridad física y ambiental 43
2.6.7 Tecnologías de la información operaciones y comunicaciones 43
2.6.8 Control de accesos 43
2.6.9 Mantenimiento y desarrollo de sistemas 44
2.6.10 Planes de continuidad del negocio 44
2.6.11 Control de adecuación a las leyes 44
3 Anexo cuestionario para la recolección de información en el Centro de Datos 45
3.1 Preguntas para los administradores 45
3.1.1 Instalaciones físicas 45
3.1.2 Conexiones y tipo de tecnología empleada para infraestructura de red 45
3.1.3 Equipos de red con los que cuenta el Centro de Datos 45
3.1.4 Equipos informáticos (servidores) con los que cuenta el Centro de Datos 45
3.1.5 Proveedores de ancho de banda 46
3.1.6 Servicios que actualmente soporta el Centro de Datos 46
3.1.7 Servicios que presta el Centro de Datos a la comunidad universitaria 46
3.1.8 Administración, instalación y mantenimiento de los equipos 46
3.1.9 Administración instalación y mantenimiento de los servicios 46
3.1.10 Estaciones de trabajo 46
3.1.11 Características de acceso a los servidores y servicios 47
3.1.12 Administración de usuarios 47
3.1.13 Planes de contingencia 47
3.1.14 Planes para realizar copias de seguridad 47
3.1.15 Planes de seguridad 47
3.1.16 Información acerca del personal 48
3.1.17 Funciones del área 48
3.1.18 Planes de continuidad 48
3.1.19 Agentes y proveedores externos 48
3.1.20 Historial de amenazas y fallos de seguridad 48
3.2 Preguntas para los usuarios 48
3.2.1 Cómo perciben la prestación de los servicios 48
3.2.2 Cómo perciben la seguridad de la información 49
3.2.3 Normas de seguridad que se deben cumplir 49
4 Guía metodológica que permite definir los criterios para establecer políticas de seguridad de la información para un centro de datos de una institución de carácter educativo 50
4.1 Presentación 50
4.2 Introducción 51
4.3 Fases para la creación de las políticas para seguridad de la información 51
4.3.1 FASE I. Inicio 52
4.3.2 FASE II. Planeación 56
4.3.3 FASE III. Establecimiento 58
4.3.4 FASE IV. Mantenimiento 61
4.3.5 CRONOGRAMA DE REFERENCIA 1 62

4.4 Anexo criterios para realización de la etapa del análisis de riesgos 63
4.4.1 Parte I. Análisis y planificación de riesgos 63
4.4.2 Actividad 1. Planeación 64
4.4.3 Actividad 2. Análisis 69
4.4.4 CRONOGRAMA DE REFERENCIA 2 71
4.4.5 Parte II. Actividad gestión de riesgos 72
4.4.6 CRONOGRAMA DE REFERENCIA 3 73
5 Plan de contingencia para el Centro de Datos 74
5.1 Acciones primarias del plan de contingencia. 75
5.2 Plan de contingencia general 78
5.2.1 Plan de contingencia para la recuperación de servicios 78
5.2.2 Recuperación del hardware en general 79
5.2.3 Recuperación de instalaciones físicas 79
5.2.4 Plan de contingencia para el personal 80
5.3 Plan de contingencia para los servicios principales 80
5.3.1 Servicio Web 80
5.3.2 Recuperación del servicio DNS 81
5.3.3 Recuperación del servicio de correo electrónico 82
5.3.4 Recuperación del servicio de Proxy-Cache 83
6 Plan de pruebas 85
6.1 Introducción 85
6.2 Pruebas de intrusión 85
6.3 Importancia de establecer un plan de pruebas 88
6.4 Criterios establecidos para el plan de pruebas 89
7 Anexo plan de pruebas 92
7.1 Desarrollo plan de pruebas 92
7.1.1 Conformación del equipo de trabajo 92
7.1.2 Límites y objetivos 92
7.1.3 Indicadores de operación 92
7.1.4 Cláusulas de confidencialidad 93
7.1.5 Actividades a realizar 93
7.1.6 Resultados de las pruebas aplicadas al Centro de Datos 94
8 Anexo recomendaciones para la implementación de las políticas de seguridad y el plan de contingencia en el Centro de Datos 105
9 Glosario 109
10 Bibliografía 111

Lista de figuras

Figura 1. 1 Modelo PDCA 9
Figura 2. 1 Proceso de análisis de riesgos 22
Figura 2. 2 Análisis de riesgos [27] 23
Figura 2. 3 Herramienta para análisis de riesgos SOBF 30
Figura 2. 4 Fases del análisis de riesgos 31
Figura 2. 5 Tipos de activos 34
Figura 2. 6 Dimensiones de valoración de los activos 35
Figura 2. 7 Taza anual de ocurrencia amenazas 37
Figura 2. 8 Informes 40
Figura 4. 1 Fases creación de políticas 52

Figura 4. 2 Equipo de trabajo 54
Figura 4. 3 Proceso análisis de riesgos 55
Figura 4. 4 Importancia de un análisis de riesgos 55
Figura 4. 5 Etapa de inicio 56
Figura 4. 6 Fase de planeación 58
Figura 4. 7 Fase de establecimiento 61
Figura 4. 8 Fase de mantenimiento 62
Figura 4. 9 Cronograma de referencia 1 63
Figura 4. 10 Actividades análisis de riesgos 63
Figura 4. 11 Procesos y actividades 64
Figura 4. 12 Actividad de planeación 69
Figura 4. 13 Actividad de análisis 71
Figura 4. 14 Cronograma de referencia tareas parte I 71
Figura 4. 15 Actividad gestión de riesgos 73
Figura 4. 16 Cronograma de referencia 3 73
Figura 6. 1 Etapas para la realización del plan de contingencia 74
Figura 7. 1 Tráfico red Interna 95
Figura 7. 2 Consumo ancho de banda 96
Figura 7. 3 Tráfico servidor Proxy 96
Figura 7. 4 Tráfico enlace principal con Emtel 96
Figura 7. 5 Tráfico enlace secundario con ETB 97
Figura 7. 6 Servicio de correo electrónico 97
Figura 7. 7 Servicio de correo electrónico 98
Figura 7. 8 Monitoreo servidores 98
Figura 7. 9 Tráfico interfaz Proxy Temis 100
Figura 7. 10 Tráfico interfaz Proxy Hiperion 100
Figura 7. 11 Tipo de ataques 103
Figura 7. 12 Destino y tipo de ataques 103

Lista de Tablas

Tabla 1. 1 Normas de seguridad familia 27000 7
Tabla 1. 2 Anexos ISO 27001 10
Tabla 1. 3 Áreas de seguridad establecidas por ISO 17799 11
Tabla 2. 1 Metodologías para el análisis de riesgos 27
Tabla 2. 2 Comparación entre las metodologías para gestión de riesgos 27
Tabla 2. 3 Herramientas para el análisis y gestión de riesgos 29
Tabla 2. 4 Comparación entre las herramientas para análisis de riesgos 30
Tabla 4. 1 Roles equipo de trabajo 53
Tabla 4. 2 Criterios para establecer políticas de seguridad 55
Tabla 4. 3 Etapas fase de planeación 57
Tabla 4. 4 Criterios fase de planeación 57
Tabla 4. 5 Criterios con base en las áreas de seguridad de ISO 17799 59
Tabla 4. 6 Etapas de referencia fase de establecimiento 60
Tabla 4. 7 Etapas fase de mantenimiento 61
Tabla 4. 8 Etapas del cronograma de referencia 1 62
Tabla 4. 9 Criterios para el estudio de la oportunidad 65
Tabla 4. 10 Determinación del alcance del proyecto 67
Tabla 4. 11 Planificación de los medios materiales y humanos 68

Tabla 4. 12 Actividad de análisis 69
Tabla 4. 13 Tareas Cronograma de referencia parte I 71
Tabla 4. 14 Actividad gestión de riesgos 72
Tabla 4. 15 Tareas cronograma de referencia 3 73
Tabla 6. 1 Etapas del plan de contingencia 75
Tabla 6. 2 Recuperación de servicios 78
Tabla 6. 3 Recuperación de hardware 79
Tabla 6. 4 Recuperación de instalaciones físicas 79
Tabla 6. 5 Plan de contingencia para el personal 80
Tabla 6. 6 Plan de contingencia servicio Web 80
Tabla 6. 7 Plan de contingencia del servicio DNS 81
Tabla 6. 8 Plan de contingencia del servicio de correo electrónico. 82
Tabla 6. 9 Plan de contingencia servicio de Proxy-Cache 83
Tabla 7. 1 Verificación de contraseñas 101
Tabla 7. 2 Detección de virus 102
Tabla 7. 3 Origen de virus 102
Tabla 7. 4 Destino de virus 103
Tabla 7. 5 Destino de los ataques 104

1 Generalidades de las normas para la seguridad de la información

1.1 Normas para la seguridad de la información

La información es un recurso vital para el adecuado funcionamiento y continuidad de cualquier empresa que haga uso de ella, su aseguramiento y el del entorno con el cual esta interactúa, es un objetivo primordial para las organizaciones. Ante esta necesidad surgen varios estándares que proporcionan un marco de gestión para la seguridad de la información aplicable a cualquier tipo de organización.

1.1.1 Normas ISO 27000

Su objetivo principal radica en la implementación y diseño de un sistema para proveer seguridad de la información, este sistema debe permitir preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información, características que le permiten a los usuarios acceder a la información en el momento que lo requieren, con la seguridad de que su información está completa y es manejada de una forma segura. Las normas de seguridad de la familia 27000 [1], se pueden observar en la tabla 1.1:

Tabla 1. 1 Normas de seguridad familia 27000

NORMA	DESCRIPCIÓN
ISO 27000	Contendrá el vocabulario y las definiciones.
ISO 27001	Estándar para gestión de seguridad de la información, ya es certificable.
ISO 27002	Código de buenas prácticas que sustituye la norma ISO 17799, no es certificable.
ISO 27003	Guía para la implementación de un sistema de gestión de la seguridad de la información.
ISO 27004	Métricas e indicadores, en desarrollo.
ISO 27005	Gestión de riesgos, en desarrollo.
ISO 27006	Continuidad del Negocio/Recuperación de desastres, en desarrollo.

1.2 Norma ISO 27001

Este estándar fue desarrollado principalmente para dar los lineamientos que permitan a una empresa implementar un SGSI[1], de tal manera que esta empresa sea autónoma y capaz de mantener los lineamientos y pautas que le permitan diseñar, implementar, mantener revisar y

[1] SGSI: Sistema de gestión de la seguridad de la información.

monitorizar su propio sistema. Por su flexibilidad permite a cada empresa adecuarlo a la necesidad propia de su negocio, de manera que la complejidad del sistema depende del negocio en sí. Una característica fundamental está en que la norma es orientada a lograr que en una organización se mejore la forma como se realiza la gestión de la seguridad de la información [2]. En términos generales los puntos claves hacia los cuales se enfoca este estándar, son:

- Implementación del SGSI.
- Gestión de los riesgos ha los cuales está expuesto una empresa.
- Controles que se pueden aplicar.

Dentro de este proceso es importante que la empresa identifique las actividades y defina cuales pueden ser consideradas como procesos, de tal forma que defina los resultados que obtendrá, para poder organizar y priorizar los mismos para ser usados de una manera adecuada y además, sirvan para realimentar otras actividades que realiza y que necesitan de los resultados de fases anteriores [2]. Esta norma invita a enfatizar en la importancia de:

- Entender la manera más adecuada de organizar la seguridad de la información, de tal manera que se puedan diseñar e implementar políticas de gestión de la seguridad de la información.
- Implementar y operar controles que permitan administrar los riesgos de seguridad de la información a los cuales se encuentra expuesta la organización, debido a las características del negocio que maneja.
- Revisar el desempeño, la efectividad y las características de funcionamiento del SGSI, los beneficios y retribuciones para la empresa, que permita continuar mejorando el desempeño y los resultados obtenidos con dicha implementación.

Para la implementación el estándar propone un modelo de procesos denominado PDCA[2], este modelo es aplicado a toda la estructura y a la implementación del SGSI, es importante mencionar que este modelo es un reflejo del OECD[3] el cual es un estándar internacional que provee un robusto modelo para la implementación y lineamientos para la medida de riesgos,

[2] PDCA: Plan –Do-Check-Act: Planear – hacer – verificar - actuar.
[3] OECD: Lineamientos para la seguridad de la información en sistemas y redes.

la seguridad, diseño e implementación de un sistema para administrar la seguridad. El modelo PDCA propone: [3]

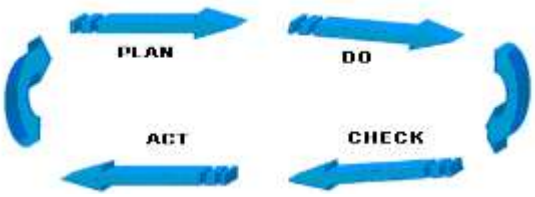


Figura 1. 1 Modelo PDCA

- **Plan:** En esta fase se establece el SGSI, para lo que se deben definir las políticas, procesos y actividades importantes que permitan administrar de una manera adecuada la gestión de riesgos, de modo que puedan ser adaptadas a las características de la organización según su negocio.
- **Do:** Implementar y operar el SGSI, en esta etapa lo que se pone en marcha son las políticas y actividades diseñadas y establecidas para lograr una adecuada gestión de la seguridad de la información.
- **Check:** Monitorizar y revisar el SGSI, en esta etapa lo que se pretende es estudiar, analizar y medir en donde se encuentren puntos de comparación de los objetivos y las políticas propuestas, para de esta manera recoger los resultados y las experiencias obtenidas para conformar un plan donde se puedan corregir y evaluar.
- **Act:** Mantenimiento y mejora del SGSI, con base en los resultados obtenidos en la fase anterior y el documento generado, así como de una auditoría interna al sistema implantado, tomar medidas correctivas y preventivas que permitan mejorar el SGSI, de manera que se pueda continuar con una mejora permanente.[4]

1.2.1 Compatibilidad con otros sistemas de gestión

La compatibilidad de esta norma es muy estrecha con otros sistemas de gestión como lo son: la norma ISO 9000 y la norma ISO 14000, donde se mantienen y emplean muchos de los conceptos claves de gestión empleados con otras normas, lo que lo hace muy funcional y estrechamente relacionado, aunque se podría pensar en que trabajan sobre áreas diferentes que los hacen poco compatibles, la realidad es que al trabajar juntos se complementan y permiten que sea mucho mejor la gestión de los recursos y la manera como estos se gestionan y administran para generar un resultado más eficiente con el sistema o negocio en el cual se está implementando.[5]

1.2.2 Sistema de Gestión de Seguridad de la Información

Es un mecanismo que al ser implementado permite diseñar y generar controles de seguridad que le permitirán a una empresa mantener y administrar la información, proporcionando y garantizando integridad, confidencialidad y disponibilidad de la información. Es una parte de un sistema de gestión global que permite a una organización poder controlar el flujo de la información que maneja, ya que permite establecer, implementar, operar, monitorizar, revisar y mantener sus actividades y mecanismos de negocio, de igual manera este sistema permite mejorar el nivel de seguridad con el que es tratada la información. Dentro de este proceso se deben destacar los activos de información, que son en el contexto de la información, las cosas que tienen valor para la organización, también las posibles amenazas a las cuales se ve expuesta una organización, las que son las posibles fuentes, acciones o mecanismos que pueden producir daños, perdidas de bienes tangibles o intangibles, estas amenazas pueden tener diferentes características y pueden verse concentradas en el exterior de la organización o distribuidas dentro de la misma organización.[6]

1.2.3 Anexos ISO 27001

Como complemento a los parámetros establecidos por la norma se tienen tres anexos, los cuales ayudan en el proceso de implementación de esta norma en una organización, a continuación se da un breve resumen de estos:

Tabla 1. 2 Anexos ISO 27001

ANEXO	DESCRIPCIÓN
A	Detalla el control de objetivos y los controles que se deben definir para el proceso de gestión de seguridad de la información y quedan agrupados y numerados de la siguiente manera: • Política de seguridad. • Organización de la seguridad de la información. • Administración de recursos. • Seguridad del recurso humano • Seguridad física y del entorno. • Administración de las operaciones y comunicaciones. • Control de accesos. • Adquisición de sistemas de información, desarrollo y mantenimiento. • Administración de incidentes de seguridad. • Administración de la continuidad del negocio. • Cumplimiento legal de estándares técnicos y auditorias.
B	Es informativo y provee un breve guía de los principios de OECD y la correspondencia con el modelo PDCA.
C	Informativo, resume la correspondencia entre ISO 9001:2000 y el ISO 14001:2004.

1.3 ISO 17799

Es un estándar internacional publicado por la ISO para la administración de la seguridad de la información, al ser definido como un guía para la implementación de un sistema de gestión de la seguridad de la información, está orientado a preservar los principios de confidencialidad, integridad y disponibilidad de la seguridad informática. La necesidad de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, dio origen a su elaboración, basado principalmente en la primera parte del BS 7799 conocido como Código de Buenas Prácticas. [7]

1.3.1 Los controles de ISO 17799

El análisis de riesgos es un requisito indispensable para el éxito en la aplicación del estándar, con el se identificarán los activos de información y las amenazas a las cuales se encuentran expuestos, a su vez orientará la selección adecuada de los controles que deban aplicarse a la organización. En la tabla 1.3 se encuentran las diez áreas de seguridad establecidas por el estándar, en donde se esclarecen los objetivos de estos controles.

Tabla 1. 3 Áreas de seguridad establecidas por ISO 17799

Política	Descripción
Políticas de seguridad	Donde se deben establecer las políticas de seguridad documentadas y los procedimientos internos para su actualización y revisión constante.
Seguridad organizacional	Para establecer las correctas bases de la gestión de la seguridad dentro de la organización.
Clasificación y control de activos	Su objetivo es inventariar los activos que deben ser protegidos.
Seguridad del personal	Orientada a proporcionar controles a las acciones del personal que opera con los activos de información.
Seguridad física y de entorno	Establecer los controles de seguridad como manejo de equipos, transferencia de información y control de los accesos a las distintas áreas de las instalaciones físicas.
Comunicaciones y administración de operaciones	Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, con el fin de asegurar la información.
Control de acceso	Definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
Desarrollo de sistemas y mantenimiento	Garantizar la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.
Continuidad de las operaciones	Establecimiento de procedimientos de recuperación en caso de contingencias.
Requerimientos legales	Análisis del cumplimiento con la legislación vigente de acuerdo a la localización territorial.

ISO 17799 no es certificable, sólo realiza recomendaciones sobre la utilización de 127 controles de seguridad aplicados en las 10 áreas de control. Pero no establece requisitos que al cumplirlos puedan certificarse.

1.4 Normas complementarias para seguridad de la información

1.4.1 ISO 13335

Directrices para la Gestión de la Seguridad (GMITS), ofrece un marco de referencia de las técnicas de gestión de riesgos y del criterio de selección de las medidas de protección. [8]

1.4.2 ISO 15408

Criterios Comunes (CC), con el objeto de reducir el nivel de riesgos conforme lo determina la norma BS 7799-2, permite seleccionar una gama de productos, a modo de medidas de protección que pueden ser certificados en los niveles de aseguramiento que proporcionan. [9]

1.4.3 ISO 21827

Ingeniería de Seguridad de Sistemas - Modelo de Madurez de Capacidad (SSE-CMM), también es un marco de referencia, en este caso respecto al nivel de madures de los procesos relacionados especialmente con los riesgos y el aseguramiento que define BS 7799-2 bajo el esquema de mejoramiento continuo del ciclo PDCA. [10]

1.4.4 BS 7799

Esta norma posee dos partes, una primera que representa el código de buenas prácticas y una segunda que son las especificaciones para la gestión de la seguridad de los sistemas de información, con la segunda parte de la norma las organizaciones que lo deseen pueden certificarse. La ISO en la actualidad está trabajando para terminar esta segunda parte del ISO/IEC 17799 con el objetivo de que las organizaciones puedan certificarse contra esta norma de carácter internacional.

Esta norma Británica presenta los requisitos para un sistema administrativo de seguridad de la información, está relacionada con la norma ISO/IEC 17799 la cual se convertirá en la ISO/IEC 27002, que provee criterios estandarizados e internacionalmente aceptados para implementar un efectivo SGSI. Así mismo define que la información es el elemento más valioso e importante que tiene una organización, por lo cual debe ser protegido de una forma completa, es decir se debe proteger de amenazas que pueden ser externas e internas. La norma define procedimientos y lineamientos que permiten que la información sea tratada de una manera adecuada. Además propone técnicas y estrategias que permiten analizar, evaluar, medir los posibles riesgos y proteger los activos de información. [11]

1.4.5 FISMA Proyecto estadounidense

FISMA[4] Ley federal de la gestión de la seguridad de la información, este proyecto fue establecido en el año 2003 y el propósito es producir estándares y guías de seguridad que permitan proteger la infraestructura de información, que por sus características es clasificada como crítica para los Estados Unidos de acuerdo a lo promulgado por el *E-government*[5], las empresas que tengan la responsabilidad de manejar las tecnologías de la información, deben cumplir con lineamientos que le permitan documentar e implementar un programa entero que ofrezca mecanismos de seguridad de la información para los activos de la empresa. [12]. La visión del proyecto está enfocada a desarrollar estándares de seguridad y lineamientos para soportar la implementación y la conformidad con la FISMA, para esto incluye:

- Estándares para categorizar la información y los sistemas de información así como el impacto.
- Estándares para requerimientos mínimos de seguridad para información y sistemas de información.
- Guías para asegurar los apropiados controles de seguridad para los sistemas de información.
- Guías para certificar y acreditar los sistemas de información.

Lo anterior está dirigido a:

[4] FISMA: Federal Information Security Management Act.
[5] E-goverment: Gobierno electrónico.

- La implementación de un sistema efectivo, teniendo en cuenta riesgos basados en los programas de seguridad.
- El establecimiento de un nivel de seguridad acorde al exigido por las empresas federales.
- Un desarrollo que sea más consistente en cuanto a lo que es infraestructura, costos y eficiencia.
- Medidas y controles de seguridad más consistentes, comparables y repetibles.
- Un entendimiento más concreto en cuanto a lo que es el negocio, los riesgos críticos para este y la manera como están operando los sistemas.
- Manejo de la información de una manera más completa y fiable, para así facilitar la toma de decisiones, cambios y la interacción con el gobierno.

1.4.6 FIPS 140-2 Ley Estadounidense

Ley de procesamiento federal de los estados unidos FIPS 140-2, define los requisitos generales para módulos de cifrado, especificando los criterios necesarios para el diseño e implementación seguro de módulos que proveen protección segura a datos que son valiosos y sensibles. Es importante mencionar que una empresa que quiera realizar algún tipo de negocio con una empresa estadounidense que maneje información, debe de manera obligatoria cumplir con esta norma.

Los requerimientos de seguridad cubren 11 áreas relacionadas al diseño y la implementación de módulos de cifrado de información, que a su vez cubren muchas más áreas, cada modulo recibe un nivel de seguridad evaluado. Estos niveles van de (1-4), del más bajo al más alto, dependiendo de que los requerimientos sean conocidos o no. Algunas áreas que no proveen diferentes niveles de seguridad reciben una evaluación que refleja completamente todos los requerimientos para esa área. [13]. En este proceso se emite una evaluación completa la cual indica:

1. El mínimo de las evaluaciones recibidas en las áreas que cuentan con más de dos niveles.
2. Realización de todos los requerimientos en otras áreas, hay que tener claro que cada área según se evalué y se determine va a tener unas evaluaciones diferentes, lo que implica que no se puede comparar una área con otra según su evaluación, ya que

hay otros factores que son muy importantes, por mencionar uno se puede hablar de un análisis de riesgos.

1.4.7 Ley Sarbanes-oxley

La ley *Sarbanes-Oxley* de 2002 (SOA), es una ley de Estados Unidos muy importante en cuanto a la legislación y a las leyes a las cuales están sujetas las empresas especialmente en el ámbito financiero, esto plantea grandes cambios y oportunidades tanto para empresas como para usuarios. Tiene como objetivo crear un ambiente de transparencia para las transacciones bancarias tanto para los bancos como para los usuarios e incluso el mismo estado, permite generar y dar solución a los posibles inconvenientes que se han presentado y han ido declinando en pocos resultados y pérdida de credibilidad, esta ley básicamente cubre las empresas estadounidenses hasta el sector financiero, sus subsidiarias en todo el mundo y las empresas que invierten en la bolsa de valores de los Estados Unidos. La ley realiza controles más concretos y profundos a los reportes y estados financieros que una empresa aporta como respaldo de los movimientos financieros de cada año, lo que se pretende con estas medidas es lograr detectar los posibles fraudes o inconsistencias, así mismo tener las bases sobre las cuales se puede aplicar los correctivos necesarios. Está sujeta y es obligatoria para algunas empresas, pero esta ley no cubre a nivel Internacional y hay empresas que deciden no aceptarla. Dentro de algunos de los requerimientos importantes que exige la ley se pueden mencionar:

- Definir nuevas funciones y responsabilidades para el comité de auditoría.
- Nuevas reglas para la conformación de los consejos de administración, para que incluyan personas ajenas al grupo de control de la empresa.
- Que los directivos acompañen los reportes con una certificación personal, incrementando responsabilidades de los directores generales y de los directores de finanzas.
- Establecer un consejo de vigilancia establecido por la SEC[6]. Definir nuevas funciones y responsabilidades para el comité de auditoría.
- Código de ética para los directivos o altos funcionarios de la organización.
- Definir un esquema de medición de control interno.
- Que los directivos certifiquen el buen funcionamiento de los controles internos.

[6] SEC: Security Exchange Comisión. Comisión de valores de los Estados Unidos.

- Verificar la certificación y los certificadores.
- Reforzar las penas por fraudes.
- Nuevos esquemas de administración de riesgos.

Por sus características esta norma es un complemento de las normas de seguridad de la información porque especifica y da los lineamientos para que se pueda llegar a cumplir con los controles mínimos que permiten administrar de una manera adecuada la información, así mismo permite mantener políticas y cláusulas que permiten aplicar controles y medidas correctivas. [14]

1.4.8 COBIT

Es una herramienta de gobierno de tecnologías de la información, que permite vincular tecnología informática y técnicas de control. Está basada en un conjunto de normas globales que permiten realizar una administración y gestión de una manera centralizada y organizada. [15]

Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnologías de información que sean de uso cotidiano para gerentes y auditores, en cuanto a los diferentes entes que intervienen se encuentran:

- La gerencia: destinada a apoyar decisiones de inversión en tecnologías de la información, realizar el control sobre el rendimiento de las mismas, analizar el costo y beneficio de la implementación de controles.
- Usuarios finales: que obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los auditores: para soportar sus opiniones sobre los controles de los proyectos, su impacto en la organización para determinar el control mínimo requerido.
- Los responsables de tecnologías de la información: quienes identifican los controles que requieren cada área.

Estándares para la gestión de seguridad de la información.

1.4.9 RFC 2196

La IETF[7] elaboró este RFC[8] denominado *Site security handbook*, este documento es una guía para los administradores de equipos y servicios que se ofrecen en Internet, brinda lineamientos y recomendaciones que pueden ser tenidas en cuenta para aplicar los elementos y correctivos necesarios para asegurar un tratamiento adecuado de la información. Ofrece los parámetros necesarios para aplicar políticas y métricas de seguridad y las recomendaciones aplican a cualquier tipo de organización independiente de los recursos que maneje o su tamaño. [16] Dentro de las etapas que recomienda seguir se tienen:

- Identificar que se está tratando de proteger (los activos).
- Identificar de quienes se está tratando de proteger los elementos, es decir identificar los riesgos.
- Identificar qué tan probable es que se materialice una amenaza.
- Implementar las medidas que puedan proteger los activos en una relación costo beneficio efectivas.
- Realizar revisiones continuas para esta manera identificar posibles debilidades sobre realidades que surgen con el tiempo.

1.4.10 Manual de protección para tecnologías de la información

Provee los lineamientos básicos para la protección de la información, este documento presenta métricas o recomendaciones para la implementación de medidas de control que ayuden a minimizar los riesgos a los cuales encuentran expuestos los elementos que constituyen los sistemas de información. Es desarrollado por la agencia de información de Alemania y es denominado *IT baseline protecction manual*. [17]

1.4.11 OECD

[7] IETF: Internet Engineering Task Force. Grupo de Trabajo de Ingeniería en Internet.
[8] RFC: Request For Comments. Petición de comentarios.

OECD[9] son lineamientos para la seguridad de la información de sistemas y redes, que enfatizan en la necesidad imperiosa de solventar las necesidades y requerimientos de seguridad que han ido surgiendo con el crecimiento de tecnologías y con la expansión de las redes y el acceso a Internet, dichos lineamientos quieren proveer y generar una cultura de la seguridad de la información, donde no se realicen estos procesos porque es necesario contener una situación anormal, sino porque son hábitos cotidianos que ayudan a mejorar el desempeño de los servicios que se prestan. [18] Dentro de los principales puntos que maneja se puede mencionar:

- Promover una cultura de seguridad de la información entre las personas involucradas y participantes de este proceso de tal manera que se puedan proteger los servicios, las redes y los sistemas.
- Generar espacios para formación en cuanto al riesgo, junto con las prácticas y procedimientos que permiten mantener los riesgos en un nivel aceptable y asimismo incrementar la calidad disponibilidad de los servicios ofrecidos.

Estándares para evaluación de seguridad en sistemas:

1.4.12 ISO 15408

Criterios Comunes, constituye un sistema reconocido para definir los requisitos de seguridad aplicables a los productos relativos a la red y a los ordenadores para comprobar si un determinado producto cumple tales requisitos. [19]

1.4.13 Serie arco iris Rainbow Series (orange books) (EE.UU)

Es un importante conjunto de documentos que delimita una serie de estándares de seguridad desarrollados para ser aplicados en Estados Unidos, de esta serie se puedan resaltar importantes libros, los más conocidos es el TSEC[10] o *Orange Book*, el cual es un documento útil para la gestión de la información. [20]

1.4.14 ITSEC Reino Unido

[9] OECD: Guidelines for the Security of Information systems and Networks.
[10] TSEC: trusted computer system evaluation criteria.

En Mayo de 1990, Francia, Alemania, Los países bajos y el Reino Unido publicaron el ITSEC[11] basado en el trabajo existente en sus respectivos países. Después de una extensiva revisión internacional, la versión 1.2 fue publicada en 1991 por la comisión de las comunidades Europeas para usos operacionales dentro de los esquemas de evaluación y certificación. Es un sistema desarrollado para validar aspectos de seguridad en las tecnologías de la información, se encarga de verificar aquello que ha sido declarado por el fabricante del producto, a través de laboratorios independientes y licenciados. Sin embargo, las declaraciones no están estandarizadas. Así, si un producto tiene una calificación ITSEC, esto no indica por sí mismo que ha sido declarado y validado en su totalidad. La validación puede haberse realizado únicamente en una parte del sistema. [21]

Estándares para desarrollar aplicaciones:

1.4.15 CMM

CMM[12] es un método para garantizar madurez en procesos. El instituto de ingeniería lidero el desarrollo de este método el cual es muy importante ya que cuenta con aspectos de seguridad que deben ser tratados en el desarrollo de un proyecto. [22]

1.4.16 SSE-CMM

SSE-CMM[13] Es un derivado del CMM, describe las características esenciales del proceso de la ingeniería de la seguridad de una organización que deben existir para asegurar la buena ingeniería de la seguridad. [23]

Estándares para servicios financieros:

1.4.17 ISO 11131

Especifica tres tipos de registro de autenticación entre las entidades que soliciten el acceso y entidades capaces de otorgar el acceso a través de Autenticación de Información Personal (PAI), como una contraseña, una clave de usuario única, una clave única de nodo. Está

[11] ITSEC: Information Technology Security Evaluation Criteria. Criterios de Evaluación de la seguridad en tecnologías de información.
[12] CMM: Capability Maturity Model.
[13] SSE-CMM: System Security Engineering Capability Maturity Model.

diseñado para su uso con algoritmos simétricos, donde solicitante y otorgante utilizan la misma clave. [24]

1.4.18 ISO 13569

Es una directiva para la seguridad de la información en servicios financieros. Esta directiva describe entre otras medidas para la administración de la seguridad, la política de seguridad para tecnologías de información, el análisis de riesgos y el plan de contingencia. Por otra parte describe la selección de controles apropiados y elementos necesarios para la gestión de riesgos. [25]

2 Anexo análisis de riesgos

2.1 Introducción

Para ofrecer e implementar mecanismos de seguridad es importante realizar un proceso previo que permita conocer los elementos más importantes para una organización, así como las necesidades y falencias que se tienen en cuanto a la seguridad de la información, es por esto que para garantizar la seguridad no sólo es necesario contar con dispositivos robustos o de última tecnología, también se debe contar con un estudio previo que permita conocer a fondo las características y la estructura de la organización que se quiere proteger, determinando los servicios, los datos, la infraestructura de red, el personal y situaciones o eventos que afectan con mayor frecuencia el normal funcionamiento de las actividades y los servicios prestados. El proceso de conocimiento de la empresa permite determinar las posibles amenazas tanto externas como internas que pueden llegar a repercutir y generar una degradación de la información y de los servicios prestados, que con el tiempo se puede traducir en pérdidas económicas y de reputación. Determinar estos elementos genera los puntos de partida para que se pueda llevar un proceso adecuado de gestión de seguridad de la información, en miras de obtener el aval o la aplicación de una norma de seguridad de la información internacionalmente aceptada

En el presente anexo se encontrarán definiciones y conceptos que ayudan en el proceso de estudio y realización de un análisis de riesgos, así mismo da las pautas para el uso de una metodología en un ambiente educativo. El resultado del análisis de riesgos desarrollado en el Centro de Datos de la Universidad del Cauca se encuentra plasmado en el capitulo dos denominado “Análisis de riesgos para el Centro de Datos”.

2.2 Definición de análisis de riesgos

Es un proceso fundamental, que debe ser realizado para garantizar una adecuada gestión de la seguridad de la información, dicho análisis comprende elementos como: los activos, que son los elementos que para la organización son importantes, que pueden ser un servidor Web, datos de transacciones, el personal entre otros, las amenazas o elementos que pueden

interrumpir el normal funcionamiento de las actividades, los planes de contingencia y los mecanismos de protección con los que se cuenta para actuar frente a situaciones no previstas. Al tener definidos de una manera clara y efectiva estos elementos, se puede estimar para la empresa el impacto que causaría la materialización de una amenaza o un riesgo sobre un activo o lo que causaría la ocurrencia de un evento inesperado.

Realizar un análisis de riesgo permite a una empresa definir puntos de partida y elementos de fondo que permiten generar y aplicar planes de contingencia para hacer frente a posibles amenazas, con este análisis y con la información definida y organizada, se puede determinar de manera aproximada lo que una amenaza podría causar a una empresa, esto ayuda a tener en cuenta parámetros que permitan realizar una adecuada gestión de la información de tal manera que se pueda garantizar la prestación de servicios ya que cumplen con los requerimientos necesarios.

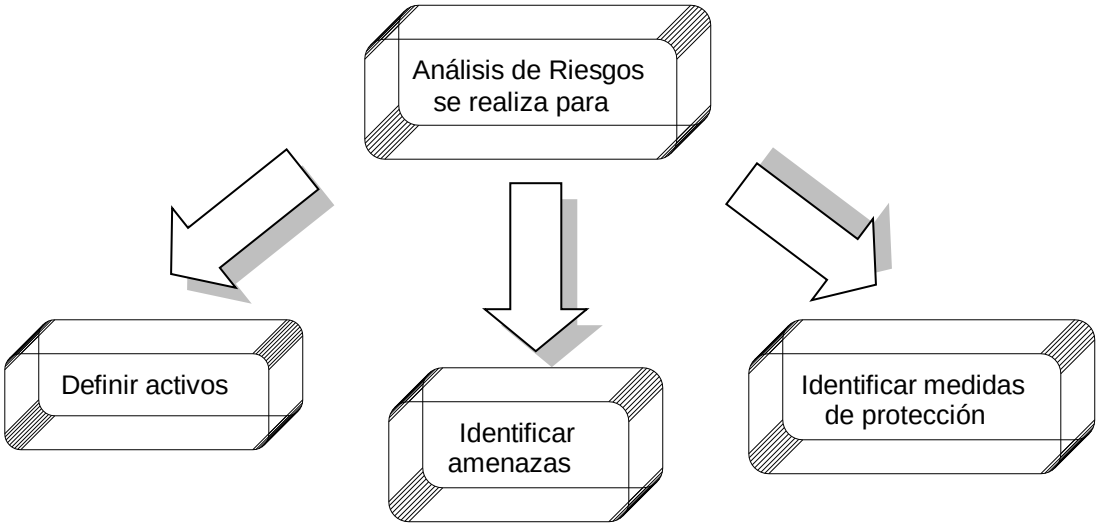


Figura 2. 1 Proceso de análisis de riesgos

El análisis de riesgos permite determinar el riesgo, para llevar a cabo este proceso se deben seguir los pasos dados a continuación:

1. Determinar los activos relevantes para la organización.
2. Valorar dichos activos en función del costo que supondría para la organización recuperarse de un fallo de disponibilidad, integridad, confidencialidad o autenticidad.
3. Determinar a qué amenazas están expuestos aquellos activos.
4. Valorar la vulnerabilidad de los activos a las amenazas potenciales.
5. Estimar el impacto, definido como el daño sobre el activo derivado de la

materialización de la amenaza.

6. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o materialización de la amenaza.

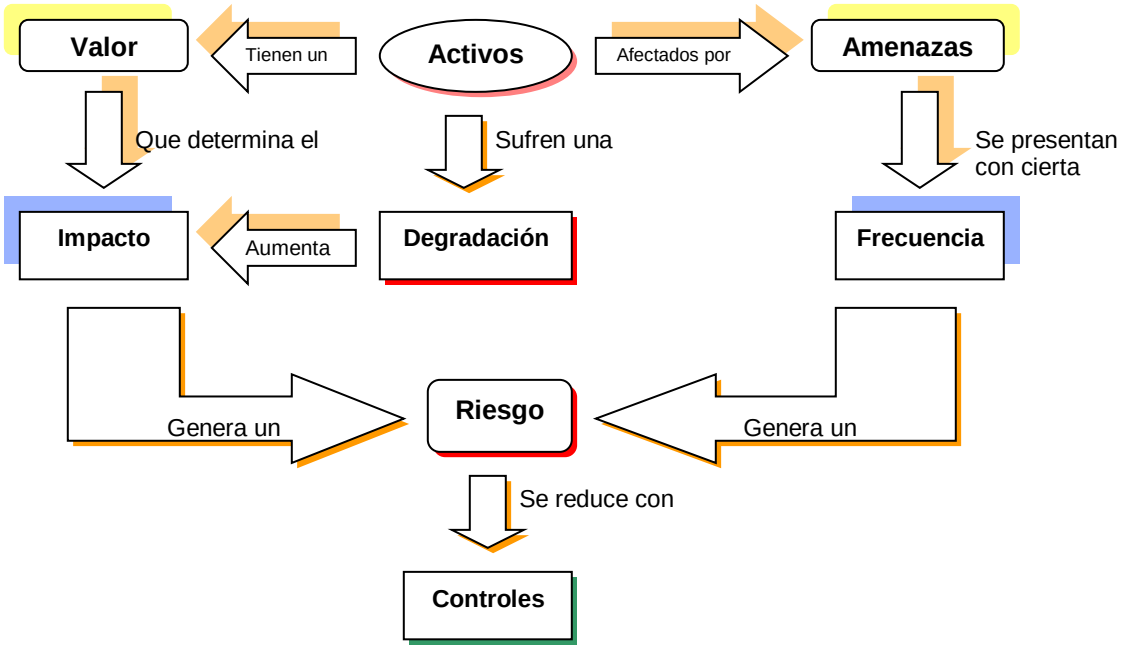


Figura 2. 2 Análisis de riesgos [27]

La gestión del riesgo es un proceso que se hace cada día, se hace lo mismo dentro de un ambiente de negocios. ¿Qué tan arriesgado es gastar dinero en una nueva herramienta de software? ¿Qué tan arriesgado es iniciar una nueva unidad comercial? ¿Qué tan arriesgado es montar un servidor Web? La totalidad del manejo del riesgo está sobre nosotros queriendo hacer algo y nosotros pensando en las consecuencias que esto puede tener. Por lo tanto la gestión del riesgo puede ayudar a decidir qué hacer y qué no hacer. [26]

La gestión del riesgo es un negocio diario, cuando se implementan medidas de seguridad y controles basados en un análisis de riesgos, esto no es suficiente para solo implementar esas medidas de seguridad, esta implementación de medidas de seguridad y controles también necesita ser revisada regularmente, tales actividades de mantenimiento incluyen [26]:

1. Análisis de archivos de sucesos del sistema.
2. Revisión de la implementación de medidas de seguridad y su efectividad.
3. Iniciar un nuevo análisis de riesgo cuando un ambiente cambie.

2.2.1 Limitaciones de la gestión del riesgo

Entonces cuando ha finalizado la gestión del riesgo, surge el interrogante sobre ¿qué no puede ser gestionado? La gestión del riesgo puede volverse muy consumidora de tiempo y por lo tanto costosa, cuando la meta es remover cada riesgo, gastar demasiado tiempo en analizar un riesgo improbable o pequeño puede volverse muy costoso. Aunque la gestión del riesgo es sobre el riesgo administrable, esta no define que riesgo tomar y que riesgo mitigar, mientras el proceso de gestión ofrece algunas herramientas y ayudas, también requiere tener algo de conocimiento previo del área y algo de experiencia. Por lo tanto siempre es una buena idea iniciar un proceso de gestión del riesgo con algún experto.

2.2.2 Estrategias para la gestión del riesgo

Hay dos posibles estrategias para gestionar el riesgo. Una estrategia pro-activa y una reactiva.

Pro-activa: Manejando el riesgo de manera pro-activa significa gestionar el riesgo “antes que algo suceda”. Esta es la estrategia correcta, debería ser así ya que esto significa buena rentabilidad y riesgo bajo.

Reactiva: Significa que hay solamente una reacción “después que algo ha ocurrido”. Esta estrategia también es conocida como apaga incendios. Reaccionar a un riesgo cuando un incidente o un ataque ocurren significa baja rentabilidad y una estrategia muy costosa.

2.2.3 Importancia de la gestión del riesgo

La gestión del riesgo no solo es importante porque se puede perder dinero o ventajas de competitividad. La gestión del riesgo también es importante por estas razones:

- La gestión del riesgo es una forma de justificar inversiones.
- La junta directiva al hacer parte de este proceso puede conocer acerca de los riesgos.
- Permite a los agentes de seguridad que participan en el proceso, tales como auditores informar al administrador sobre las posibles situaciones que se puedan

estar presentando.

- Ayuda a confiar en los sistemas de información, ya que se incrementa el nivel de seguridad de la información.
- La gestión del riesgo puede ser usada como evidencia para un SGSI. Tal sistema puede ser requerido para regulación, auditorias o como precedente cuando un desastre ocurre.
- La gestión del riesgo debe ser practicada cuando una compañía se está certificando. Así mismo hay muchas razones por las cuales la gestión del riesgo es importante, estas razones cambiarán de situación a situación.

2.3 Metodologías para el análisis de riesgos

Emplear alguna de las metodologías propuestas como Magerit o SOMAP, para realizar un análisis de riesgos permite determinar de una manera sistemática y ordenada como es, cuanto vale y que tan protegidos se encuentran los activos en conjunto con los objetivos, estrategias y políticas de la organización, además ayuda a elaborar un plan de seguridad que al ser implantado y operado, permite cumplir con los objetivos propuestos en cuanto a seguridad de la información. Existen a nivel de seguridad de la información y desarrollo de software algunas metodologías, las cuales son guías que permiten utilizar procesos y lineamientos que facilitan el análisis de riesgos, de tal manera que permiten detectar en gran medida las falencias de seguridad y aspectos importantes de esta temática.

2.3.1 SOMAP

El manual de administración de riesgos de seguridad de la información SOMAP[14], contiene descripciones y explicaciones de como planear, implementar y administrar una estrategia de riesgo de seguridad de la información y actividades del SGSI. SOMAP.org es una organización suiza sin ánimo de lucro cuyo objetivo es desarrollar un proyecto abierto de la administración de riesgos de seguridad de la información y mantener documentos y herramientas libres y abiertas para agentes de seguridad y otras partes interesadas. Este contiene la información y los conceptos necesarios para la administración del riesgo,

[14] SOMAP: Security Officers Management and Analysis Project. proyecto de análisis y administración de agentes de seguridad

definiendo que es un riesgo y que se puede hacer para contar con un sistema de administración de riesgo en la organización.

SOMAP es un proyecto que actualmente trabaja sobre la herramienta SOBF[15], que permite sistematizar el proceso de gestión de riesgos, está escrita en Java y contiene una base de datos y campos para introducir activos, amenazas, vulnerabilidades, contramedidas y mapas con un inventario. SOBF brinda la posibilidad de realizar un análisis de riesgo cuantitativo y cualitativo obteniendo resultados como daños económicos, simple pérdida de expectativa, perdida de expectativa anual, etc. Los datos así como los resultados pueden ser exportados en diferentes formatos (pdf, html y otros). [26]

2.3.2 Magerit

Su principal objetivo está relacionado con el buen uso de los sistemas electrónicos, y la confianza que se le debe brindar a cada cliente, para que pueda ofrecer un servicio óptimo y de mucha calidad, los objetivos y beneficios que se esperan con el uso de esta metodología son:

- Crear conciencia en las personas encargadas de la administración en cuanto a la importancia de conocer los riesgos de seguridad a los que se enfrenta y la manera como se pueden ofrecer servicios con un nivel de seguridad más alto.
- Ofrecer un método y una metodología para el análisis de riesgos
- Ofrecer los medios y las herramientas para mantener los riesgos bajo control.
- Preparar a la organización para que pueda en un futuro enfrentarse a una posible acreditación o certificación por parte de los sistemas de información.[27]

Se tienen otras metodologías y herramientas que permiten realizar este proceso de análisis de riesgos, la gran diferencia radica en que algunas han sido diseñadas a medida para un caso especifico y son propiedad de la empresa que las desarrolla y no son de libre distribución, a continuación se consignan las más relevantes en la tabla 2.1:

[15] SOBF: Security Officers Best Friend.

Tabla 2. 1 Metodologías para el análisis de riesgos

Nombre	Descripción
Análisis y modelado de amenazas	Es una metodología desarrollada por Microsoft para el análisis y modelado de amenazas, está basada en un trabajo conjunto entre Microsoft y @stake.[28]
CORAS	Proyecto creado por la unión europea con el objetivo de proporcionar un Framework[16] donde la seguridad es crítica, para facilitar el descubrimiento de vulnerabilidades de seguridad, inconsistencias y redundancias. Para realizar el análisis de riesgos proporciona un método basado en modelos [46].
TRIKE	El propósito de la metodología es permitir describir de forma completa y precisa las características de seguridad de un sistema o de alguna organización.[30]
PTA[17]	Desarrollado por la empresa PTA, surge por la necesidad de complementar algunas inconsistencias que se tienen de la metodología inicial propuesta por Microsoft.[31]
SOMAP[18]	Proyecto de análisis para la administración de la seguridad de la información. Es una guía que describe y explica como planear, implementar y administrar una estrategia del riesgo de seguridad de la información y las actividades de un sistema de gestión de seguridad de la información, y se apoya en una herramienta que permite agilizar este proceso.[26]
OCTAVE	Metodología de evaluación de riesgos desarrollada por el SEI[19]. Incluye OCTAVE-S, una versión para pequeñas empresas.[32]
MEHARI	Método de análisis y gestión del riesgo desarrollado por el *Clusif (*Club Francés *de* seguridad de la información).[32]
EBIOS	Metodología de gestión de riesgos de seguridad en sistemas de información, desarrollada por la "Dirección central de seguridad de sistemas de información francesa.[32]

Como se puede observar se encuentran numerosas metodologías y herramientas para el análisis y gestión de riesgos, cada una de estas explota diferentes características o realiza el análisis de riesgos desde diferentes puntos de vista y se acoplan a diferentes entornos de la organización, además de que algunas de estas son ofrecidas por empresas que brindan soporte para la utilización de las mismas. Es importante destacar que cada metodología busca mejorar los resultados y niveles de seguridad para llevar el riesgo a una expresión mínima según sea las características de las empresas.

Tabla 2. 2 Comparación entre las metodologías para gestión de riesgos

NOMBRE	COMPATIBILIDAD CON LA METODOLOGÍA UTILIZADA	TIPO DE USO
Magerit	SI	Libre
Somap	SI	Libre
@stake	NO	Propietaria
CORAS	NO	Propietaria
TRIKE	NO	Propietaria
PTA	NO	Propietaria
OCTAVE	NO	Propietaria
MEHARI	NO	Propietaria

[16] FRAMEWORK: Interfaz de usuario.
[17] PTA Practical threat analysis: Análisis practico de amenazas.
[18] SOMAP: Security Officers Management Analysis Proyect: Proyecto de análisis y gestión de agentes de seguridad
[19] SEI: Software Engineering Institute: Instituto de software e ingeniería

Entre las metodologías se destacan dos de las más importantes como lo son MAGERIT y SOMAP, las cuales acorde al estudio realizado para gestión de la seguridad de la información ayudan a generar y dar los lineamientos para cubrir los objetivos propuestos para el análisis de riesgos realizado con el fin de definir las principales falencias de seguridad que se tienen. Por un lado estas metodologías permiten ser adoptadas e implementadas según las características propias del Centro de Datos, por otro lado los lineamientos sugeridos ayudan a identificar las necesidades, además permiten acoplarse a un estándar internacional como es el ISO 17799. Este proceso está enfocado a generar los pasos iniciales para una posible certificación en seguridad de la información.

Entre estas es conveniente usar MAGERIT debido a la claridad y profundidad con que manejan los conceptos sugeridos en estos procesos, además permite realizar un análisis de riesgos de una manera muy precisa, esta metodología permite a una empresa determinar todos sus activos, al seguir los pasos y los ejemplos que ofrece, y se puede llegar a obtener datos completos y entendibles de los elementos importantes y de su clasificación según sea las características del negocio, así mismo permite identificar las amenazas y la valoración que se le puede dar a ellas, es importante denotar que la metodología no puede cubrir todas las amenazas pero ofrece estándares con una aproximación muy cercana a las necesidades. Para una institución educativa los pasos propuestos por esta metodología presentan una aproximación de los aspectos más importantes a tener en cuenta para realizar un análisis de riesgos. Es importante destacar la organización que la guía presenta para la entrega de documentos y elementos necesarios para realizar este proceso.

2.4 Herramientas para el análisis y gestión de riesgos

Las herramientas son muy útiles ya que ayudan a disminuir el trabajo que toma generar informes y plantillas de una manera manual, ya que es un proceso dispendioso y largo, esto se puede comprobar al seguir paso a paso la metodología propuesta por Magerit, las herramientas al tener las plantillas y realizar los cálculos permiten ahorrar mucho tiempo y recursos, aunque tienen sus inconvenientes ya que la mayoría son propietarias y no son de libre distribución, para poder hacer uso se requiere de la adquisición de un paquete de software. En la tabla 2.3 se muestran algunas de las más conocidas [47]:

Tabla 2. 3 Herramientas para el análisis y gestión de riesgos

NOMBRE	DESCRIPCIÓN
EAR.	Soporta el análisis y gestión de riesgos siguiendo Magerit, esta herramienta se basa en la importancia, y en el hecho de que los activos están expuestos a amenazas, que cuando se materializan degradan el activo produciendo un impacto. [33]
RISKWATCH	Es una herramienta que permite realizar un análisis de riesgo de una manera fácil, hace un análisis y una detección de vulnerabilidades, basados en los lineamientos de la norma BS 17799 y NIST 800-26.[34]
CALLIO.	Callio Secura 17799 es un producto de Callio Technologies. Es una herramienta Web con soporte para bases de datos que permite a los usuarios realizar una gestión del sistema de administración de seguridad de la información, su diseño y funcionalidad está basada en los estándares ISO 17799 e ISO 27001. [35]
CASIS.	Es un analizador de trazas o huellas para realizar una auditoría inteligente, su propósito es coleccionar el registro de sucesos del sistema o de múltiples sistemas, para de esta manera unificarlos y producir un informe y generar alarmas de seguridad con base en reglas previamente definidas.[36]
COBRA.	Es una aplicación para la administración de riesgos desarrollada por *C&A System Security*. Puede ser usada para identificar las amenazas y vulnerabilidades, con base en estas generar las posibles medidas de seguridad y de contingencia que evitarán el impacto generado por la materialización de una amenaza.[37]
COUNTER MEASURES.	Desarrollada por productos ALLIONS, esta herramienta realiza la administración de riesgos basado en la serie US-NIST 800 y OMB de la circular A-130 del estándar norteamericano.[38]
CRAMM.	Esta herramienta proporciona los medios para la implementación del método Cramm, es desarrollado por Insight Consulting, El método proporciona tres niveles los cuales son totalmente soportados por la herramienta [39].
EBIOS.	Desarrollada por la división de seguridad del sistema central de información de Francia, teniendo en cuenta el soporte para el método EBIOS.[32]
GSTOOL.	Desarrollada por la BSI, la oficina federal para la información británica. Para proporcionar soporte del manual básico para proteger las tecnologías de la información (*IT Baseline Protection Manual*).[32]
ISAMM.	Herramienta para administración de riesgos desarrollada por TELINDUS, con base en las características de cada negocio y los datos suministrados genera posibles planes de contingencia y situaciones de fallos de seguridad en las cuales se puede ver avocada una empresa, para este proceso todas las acciones relevantes son organizadas sobre las bases de ROSI que es el retorno en inversiones de seguridad [32].
OCTAVE.	*Octave Automated Tool* ha sido desarrollada e implementada por la ATI[20] para ser un soporte y ayuda de los usuarios en la implementación de Octave y Octave-S. La herramienta asiste al usuario durante la fase de colección de datos, organiza la información y finalmente produce el estudio de reportes. [32]
PROTEUS.	Proteus enterprise es un producto de INFOGOV, por sus características y los componentes que emplea el usuario puede desempeñar y obtener una análisis de acuerdo a la norma ISO 17799 o crear y administrar un SGSI de acuerdo a la ISO 27001 (BS 7799-2). [42]
RA2.	Arte del riesgo dos, es una herramienta para administración de riesgos basado en los estándares ISO 17799 y la ISO 27001. Para cada etapa del proceso se generan reportes y resultados los cuales son accesibles por los usuarios. Tiene un elemento adicional denominado dispositivo para recolección de información, el cual puede ser instalado en cualquier parte de la organización para recoger información de los procesos. [43]
@RISK.	Herramienta software para realizar análisis de riesgos, por sus características de diseño permite realizar un análisis sencillo ya que su comportamiento y estructura permite obtener reportes de poca complejidad, que se pueden analizar rápidamente, esta herramienta genera graficas y funciona completamente sobre Excel, además que permiten realizar un análisis más práctico para el usuario final.

[20] ATI Advance Technology Institute: Instituto de tecnología avanzada

SOBF.	*The security officer Best Friend tool*, desarrollado bajo el proyecto SOMAP.org, es un proyecto que trata de dar los lineamientos e información detallada para un proceso de análisis de riesgos, esta herramienta se soporta sobre dos metodologías para realizar un análisis de riesgos los cuales son el método cuantitativo y el método cualitativo. [44]

Tabla 2. 4 Comparación entre las herramientas para análisis de riesgos

NOMBRE	COMPATIBILIDAD CON LA METODOLOGÍA UTILIZADA	TIPO DE SOFTWARE
SOBF	SI	Libre
TAM	NO	Gratis
EAR	SI	Propietaria
Riskwatch	NO	Propietaria
CALLIO	NO	Propietaria
COBRA	NO	Propietaria
CRAMM	NO	Propietaria
CASIS	NO	Propietaria

Con base en el estudio realizado se determinó emplear como soporte adicional la herramienta SOBF desarrollada por el proyecto SOMAP, ya que está enfocada a cumplir con los lineamientos propuestos en MAGERIT y su licencia de uso es de libre distribución, lo que permite aplicarla de manera completa aunque esta en continuo desarrollo y todas sus funcionalidades no están habilitadas. La herramienta TAM ofrecida por Microsoft está totalmente desarrollada en sus funcionalidades pero su enfoque esta dado única y exclusivamente para el desarrollo de aplicaciones software. Para el análisis de riesgos no es obligatorio el uso de una herramienta, pero al usarla se puede mejorar y reducir notablemente el tiempo empleado en la gestión de elementos y generación de reportes.

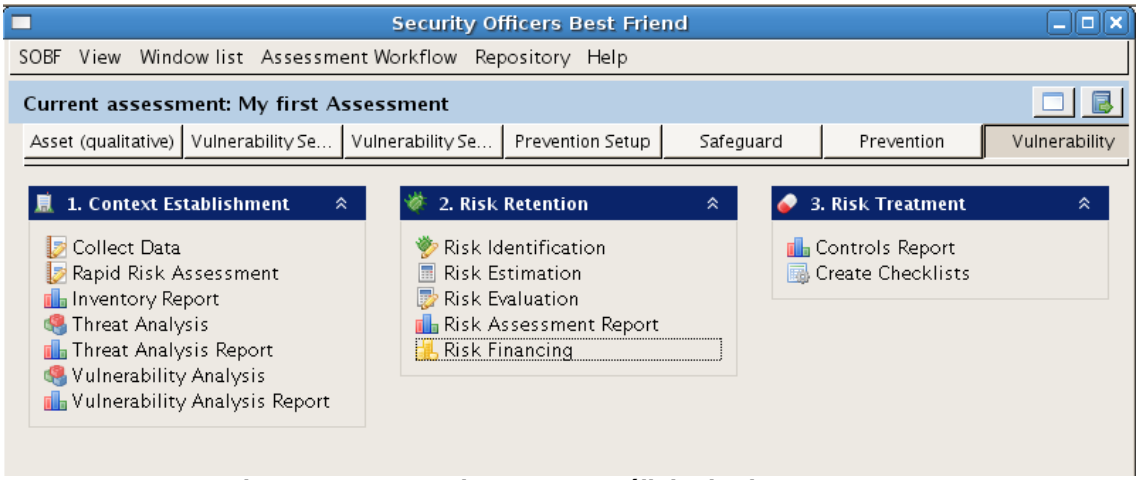


Figura 2. 3 Herramienta para análisis de riesgos SOBF

2.5 Aplicación de una metodología de análisis de riesgos en una institución educativa

Para una institución educativa el uso de las recomendaciones propuestas por la metodología Magerit [27], es de gran utilidad, ya que dicha metodología presenta de una manera amplia los puntos que se deben tener en cuenta para un proceso de análisis de riesgo, además que son tratados de una manera extensa que permite emplear los que más se adapten a las características de una institución educativa para los cuales no es tan importante algunos ítems que si lo son para una empresa, por eso a manera de ejemplo en el análisis de amenazas sin duda alguna tratar de enumerarlas seria un trabajo arduo que seguramente no tendría fin y por otra parte seria muy difícil evaluar su eficacia, pero si se toman las amenazas más probables que se tienen estandarizadas dicha tarea será más realizable y los resultados serán mejores. Para profundizar más en el tema se describen a continuación las diferentes fases que permiten realizar un análisis de riesgo.

2.5.1 Fases del desarrollo

Para el desarrollo se proponen tres fases principales con las cuales se espera obtener los mejores resultados para llevar a cabo el proyecto de una manera organizada y cubriendo la mayor parte de aspectos posibles.

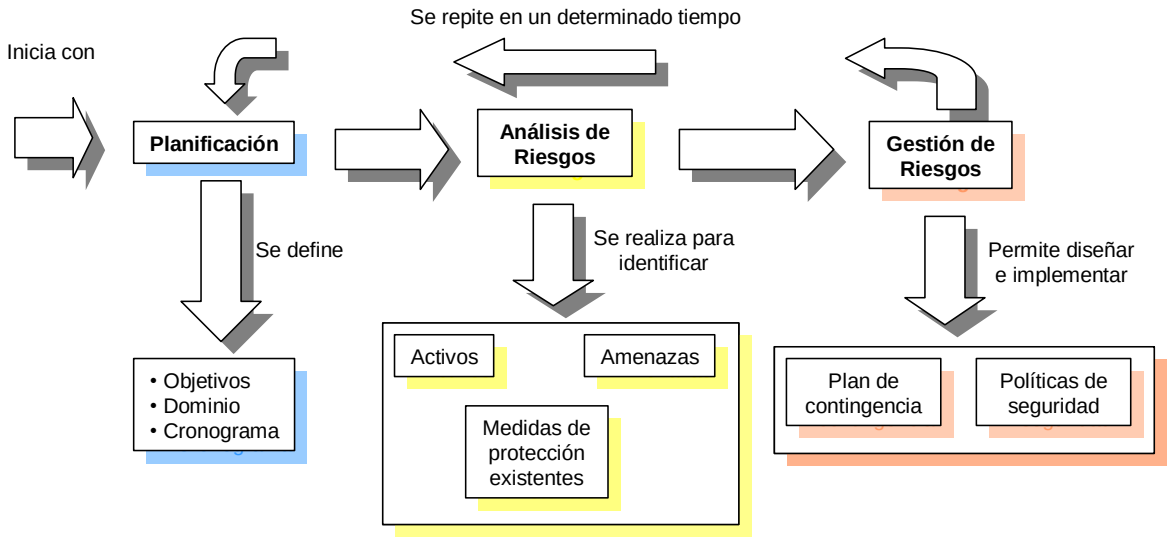


Figura 2. 4 Fases del análisis de riesgos

Fase de planificación:

En esta fase se establecen las consideraciones necesarias e importantes para que el proyecto pueda iniciar, se investiga la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el dominio que abarcará, se realiza una planificación de los medios materiales y humanos para su realización y se procede al lanzamiento del proyecto. Es importante que en esta fase se tengan en cuenta aspectos de la institución que permitan dimensionar y definir la real importancia del análisis, porque puede ser necesario realizarlo, pero respecto al tipo de información que se maneja tal vez el costo de la realización no cubra las expectativas sea demasiado alto para asumirlo, sin duda alguna delimitar el alcance y concienciar de la necesidad de este proceso es una tarea necesaria, siendo esta última muy ardua y su realización se retribuirá en mejores resultados ya que se cuenta con el apoyo del personal.

Fase de análisis de riesgos:

En esta fase se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen, se identifican las amenazas significativas sobre aquellos activos que se deben valorar en términos de la frecuencia que ocurra y la degradación o disminución que pueden causar sobre los activos, se identifican las medidas de protección existentes y se valora la eficacia de su implantación, y se estima el impacto y el riesgo residual al que están expuestos los activos del sistema. Así mismo se interpreta el significado del impacto y el riesgo, para según esto obtener una visión y una imagen de la organización.

Del análisis realizado al Centro de Datos es importante definir ciertos aspectos que se van a tratar, porque al ser una institución de carácter educativo las prioridades cambian, así mismo la importancia de los activos, conviene identificar los activos y servicios más importantes y sobre ellos iniciar el análisis, determinar con base en el tipo de información, la importancia poder darle un valor y el impacto económico, académico, para realizar esto es conveniente usar cuestionarios con los cuales se pueda recolectar información de los directos implicados en la administración de la información, dichos cuestionarios se deben realizar considerando aspectos que son relevantes para que los usuarios puedan hacer uso de Internet.

Fase de gestión de riesgos

La metodología propone una tercera fase en la cual los riesgos, que se han encontrado tienen que ser contrarrestados, es decir deben emplear mecanismos que permitan minimizar estas posibles amenazas. Se elige una estrategia para hacer frente a los riesgos identificados y al impacto que generan, definiendo medidas de protección oportunas, determinando la calidad necesaria para las medidas de protección implementadas. En esta fase se diseña un plan de seguridad (plan de acción o plan director) que permita que el impacto y los riesgos puedan ser llevados a niveles muy bajos, por último se debe realizar e implementar el plan de contingencia y el plan de seguridad, el cual debe ir acorde con los objetivos propuestos y las necesidades de la institución.

Para una institución educativa dada las características de la información que maneja se deben cubrir los siguientes tópicos de tal manera que se cumpla con los requerimientos mínimos, algunos se pueden saltar o no es necesario que se cumplan con mucha profundidad, eso depende de las características de la información y el alcance y la necesidad para dicha institución.

2.5.2 Activos

En el caso de los sistemas de información el activo más importante son los datos o la información que ellos manejan, la cual mantienen en forma digital, almacenada en cintas magnéticas, discos compactos o de almacenamiento. Pero esta no es la única clasificación de los activos, ya que se pueden definir y manejar de la siguiente manera:

a) Tipos de activos:

Se pueden clasificar dependiendo de sus características, es decir, de tipo personal, confidencial o reservado, de acuerdo a la clasificación que tengan en la institución. La metodología propone la siguiente clasificación para los activos, dependiendo de las características y el tamaño de la institución algunos pueden encontrarse y otros no esto se puede observar en la figura 2.5, para el caso de un centro de datos resulta muy útil esta clasificación ya que permite englobar casi la totalidad de elementos que los conforman.

Name	Description
Aplicaciones Software	La red de datos cuenta con u...
Datos	Para ese caso particular la inf...
Equipamiento Auxiliar	El centro de datos cuenta co...
Hardware	EL centro de datos de la univ...
Instalacione Fisicas	Actualmente el centro de dat...
Personal	Las personas que realizan la ...
Redes de Comunicaciones	Para el núcleo de la infraestr...
Servicios	Los servicios son funciones ...
Soportes Información	Actualmente el centro de dat...

Figura 2. 5 Tipos de activos

En general para una institución, la importancia radica en los servicios y la información que esta manipula, ya que por lo general ofrecen servicios como el acceso a Internet el servicio Web y el de correo electrónico. En este proceso es necesario identificar que elementos pertenecen a la institución y que elementos son contratados con otro ente, ya que según esta información se puede delimitar o enmarcar el ámbito del proyecto, si por ejemplo el servicio de correo y el Web lo maneja una empresa independiente muy seguramente dicha empresa será la responsable de la administración del mismo, mientras que si es responsabilidad de la institución esta debe emplear los mecanismos necesarios para administrarlo.

Los servicios son activos que pueden aparecer como: servicios finales prestados a terceros, servicios instrumentales donde la organización cuenta con los propios medios o como servicios contratados donde se paga a terceros por la prestación de los mismos, de igual manera pueden aparecer servicios públicos, empresariales y servicios internos.

b) Dependencias entre activos:

Es evidente que cada activo de información se ve afectado por otro activo, en ocasiones activos que se consideran menos importantes al ser afectado o impactados, su daño se retribuye en una consecuencia enorme sobre los activos considerados como muy importantes para una organización, por esto se debe determinar y tener claro la dependencia entre activos. De esto surgen los términos de activos de orden superior y los activos de orden inferior, a pesar de ser denominados de un orden menor estos activos se podría decir

que son los activos de los cuales se fundamentan los activos de información, la dependencia entre activos se puede denominar u organizar en capas. Es importante este concepto ya que se debe considerar los aspectos de una manera muy precisa, no se pueden tomar decisiones relativas sin antes realizar un proceso, porque fácilmente se puede definir como que un equipo no es importante porque puede ser reemplazado con facilidad, pero el fallo de este puede ocasionar perdida de información.

c) Valoración de los activos:

Es importante determinar el valor que cada activo representa o tiene para la institución, según su importancia o el nivel de relación que tenga con el aspecto económico o administrativo, ya que definiendo su valor real se puede determinar cuál es la verdadera importancia de este. Es necesario definirlo para tener una idea clara de cómo se verán afectados y que tan grande es el nivel de pérdidas para la organización.

d) Dimensiones de los activos:

Es importante mencionar algunas características útiles para su clasificación y valoración, como las que se muestran en la figura 2.5.

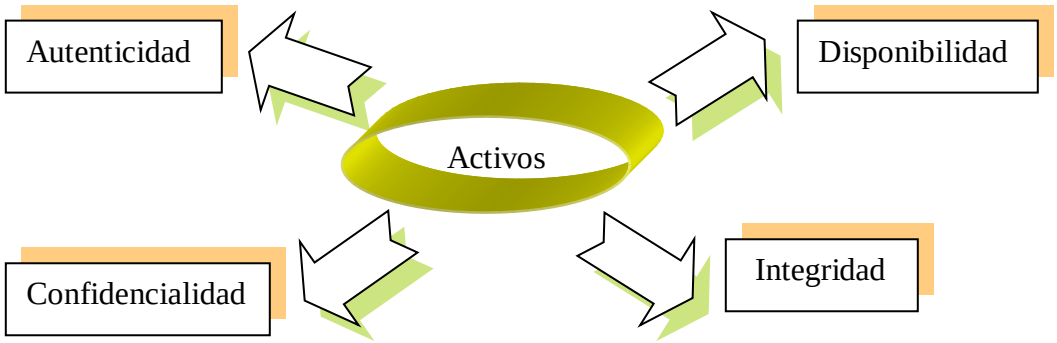


Figura 2. 6 Dimensiones de valoración de los activos

Indudablemente estas dimensiones son muy importantes, a pesar que su función principal no es la de obtener un lucro ya que en el caso de una institución garantizar a los usuarios docentes y estudiantes que sus datos son auténticos, estar seguros de su integridad y confidencialidad es un aspecto que cobra demasiada importancia y se convierte en una necesidad, no se debe olvidar que los datos se encuentran expuestos a ataques y lo que es peor provienen desde adentro de la misma institución, porque hay muchos estudiantes

curiosos dispuestos a realizar pruebas y análisis en ocasiones para aprender, pero en otras para realizar acciones no permitidas que pueden ocasionar daños. Otra dimensión importante es determinar, el valor que puede tener la reposición de un activo en un tiempo determinado, es decir la reposición de este activo cuando faltan algunos de sus componentes o cuando estos se ven afectados por un daño externo, para realizar este análisis se deben considerar muchos factores como:

- Costo de reposición.
- Costo de la mano de obra.
- Lucro cesante pérdida de ingresos.
- Capacidad de operar.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos propios o ajenos.
- Daño a personas.
- Daños medioambientales.

Este análisis se puede realizar por diferentes métodos, pero no se debe olvidar tener un punto de comparación, es decir un punto donde se pueda realizar una medida, la cual es muy importante porque contar con referencias de medida permite crear una imagen del comportamiento de la empresa.

e) Homogeneidad

Es importante que se logre o se encuentren puntos de comparación entre los diferentes activos determinados, con valores diferentes de tal manera que se pueda realizar comparaciones y se puedan tener en cuenta los activos que dependen de ellos para así conseguir una escala de la medida que permita ubicar el impacto.

f) Relatividad

Se hace necesario encontrar un nivel de dependencia y comparación de un activo en relación a otro de tal manera que se puedan hallar sus características en función del decremento de otro.

g) Disponibilidad de un servicio

Es importante tener en cuenta que los servicios dependen de su tiempo de funcionamiento, estos a su vez dependen de las características de los activos y el funcionamiento de los mismos, ya que se encontraran activos que no permiten que se esté fuera de servicio o se tendrán activos que tienen cierta tolerancia ante estas situaciones. De todas formas la disponibilidad de un activo en muchas ocasiones garantiza el funcionamiento de la empresa.

2.5.3 Determinación de las amenazas

Lo siguiente es determinar las cosas que pueden ocurrir y pueden afectar el normal desempeño de los activos, dentro de estos eventos o situaciones inesperadas se pueden obtener daños por condiciones físicas o medioambientales las cuales en ocasiones son un poco difícil de prever y están de una manera pasiva, así mismo es importante determinar los daños causados por ataques malintencionados los cuales pueden repercutir en enormes pérdidas.

- **Valoración de las amenazas**

Cuando un activo o recurso importante es afectado, no se ve afectado en todas sus dimensiones o en toda su cuantía, por lo tanto es importante determinar y estimar cuan vulnerable es el activo en los dos sentidos, determinar la degradación para determinar cuán perjudicado resulta el activo y medir el daño causado por un incidente en el supuesto de que ocurra y la frecuencia para determinar cada cuanto se materializa la amenaza. La cual se puede modelar como una tasa anual de ocurrencia siendo valores muy comunes:

Tasa	Descripción
100	Muy frecuente a diario
10	Frecuente mensualmente
1	Normal una vez al año
1/10	Poco frecuente cada varios años

Figura 2. 7 Taza anual de ocurrencia amenazas

Es importante para esto basarse en el historial de amenazas o incidentes con el que cuenta la institución, para de esta manera poder clasificarlos, la escala anterior es muy flexible y puede ser determinada según se acople a las necesidades, si no se tiene se puede recurrir a una encuesta a ciertos sectores como los usuarios, administradores. En el anexo tres se

puede encontrar más información sobre las encuestas realizadas para obtener esta información.

2.5.4 Determinación del impacto

El impacto es el daño asociado a la materialización de una amenaza, el impacto se puede calcular conociendo el valor de los activos y la degradación que causan las amenazas.

- **Impacto acumulado**

Este se calcula sobre un activo teniendo en cuenta, su valor acumulado el cual consiste en el valor propio, sumando el valor de los activos que dependen de él y las amenazas a las que está expuesto. El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración siendo una función del valor acumulado y la degradación causada. Dicho impacto puede aumentar o disminuir dependiendo de factores como: el valor propio o acumulado de un activo, cuanto mayor sea la dependencia del activo atacado mayor será la degradación de este.

- **Impacto residual**

El impacto residual se calcula teniendo como referencia un nivel de degradación más pequeño, este impacto hace referencia a las posibles situaciones en las cuales las medidas de protección no son completas o se tienen que aceptar situaciones las cuales no se pueden cubrir por completo, la sumatoria de estas situaciones imprevistas va generando un impacto residual. El cálculo del impacto residual es sencillo, como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación, la magnitud de la degradación tomando en cuenta la eficacia de las medidas de protección, es la proporción que resta entre la eficacia perfecta y la eficacia real. Este puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.5.5 Determinación de un riesgo

El riesgo es la medida probable de daño sobre un activo o sistema, conociendo el impacto de

las amenazas sobre los activos y la frecuencia de ocurrencia se puede determinar el riesgo. El riesgo crece con el impacto y con la frecuencia.

- **Riesgo acumulado**

Es el calculado sobre un activo teniendo en cuenta el impacto acumulado y la frecuencia de la amenaza, este se debe calcular para cada activo en cada amenaza y en cada dimensión de valoración siendo una función del valor acumulado, la degradación causada y la frecuencia de las amenazas, esto permite determinar las medidas de protección con las que hay que dotar los medios de trabajo

- **Riesgo repercutido**

Es el calculado sobre un activo teniendo en cuenta el impacto repercutido y la frecuencia de la amenaza, se debe calcular para cada activo en cada amenaza y en cada dimensión de valoración siendo una función del valor acumulado, la degradación causada y la frecuencia de las amenazas, además permite determinar los niveles de riesgo que son aceptados en la organización.

2.5.6 Determinación de medidas de protección

El análisis anterior mide el impacto de los riesgos sobre los activos si estos no fueran protegidos de ninguna manera. Por lo tanto se definen las medidas de protección como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, dependiendo de las características de las amenazas se encuentran las que no necesitan o se resuelven con una buena organización, hay las que necesitan la introducción de elementos tecnológicos y las que requieren la implementación de políticas de seguridad para poder llevar a cabo un adecuado tratamiento. La implementación de estos mecanismos ayuda a que se reduzca la frecuencia de las amenazas con medidas de protección preventivas, las ideales llegan a impedir que el riesgo se materialice o se limite el daño causado. Hay unas que permiten detectar las posibles degradaciones y otras permiten detectar inmediatamente el ataque para evitar la degradación. también tienen ciertos atributos y medidas que las caracterizan, lo ideal es plantear e implementar medidas de protección 100% eficaces, una medida de protección que cumpla con estas características implica cumplir con: ser teóricamente

idónea, estar perfectamente desplegada configurada y mantenida, ser empleada siempre, contar con procedimientos claros de uso normal y en caso de incidencias, tener usuarios formados y conscientes de la importancia de emplear controles y mecanismos de protección en sus lugares de trabajo, además contar con controles que avisan sobre posibles fallos.

- **Tipos de medidas de protección**

Buscan que un incidente no ocurra o que su daño sea despreciable, es decir lo importante es impedir que los ataques o incidentes se puedan materializar. Es importante tener claro que todo no se puede cubrir o garantizar en su totalidad, es decir se deben aceptar niveles de riesgo, así mismo se debe tener en cuenta que según la naturaleza del negocio hay amenazas que es muy difícil de cubrir, ya que económicamente representan un gran gasto para la empresa. Tener medidas preventivas y medidas correctivas con el tiempo generan una degradación de los activos de tal manera que se deben tener medidas que permitan recuperar los activos que se han ido deteriorando o disminuyendo. De esta manera podemos encontrar diversos tipos de medidas de protección: Medidas de protección técnicas, físicas, de organización, de personal.

2.5.7 Documentación a entregar para el análisis de riesgos

Cuando se realizan estos procesos es muy conveniente realizar las etapas con una adecuada documentación, de tal manera que se pueda contar en un momento dado con una base teórica que sirva de apoyo y de realimentación a fases posteriores y en procesos de revisión, los documentos generales o recomendados para tener en cuenta en cada fase del análisis.

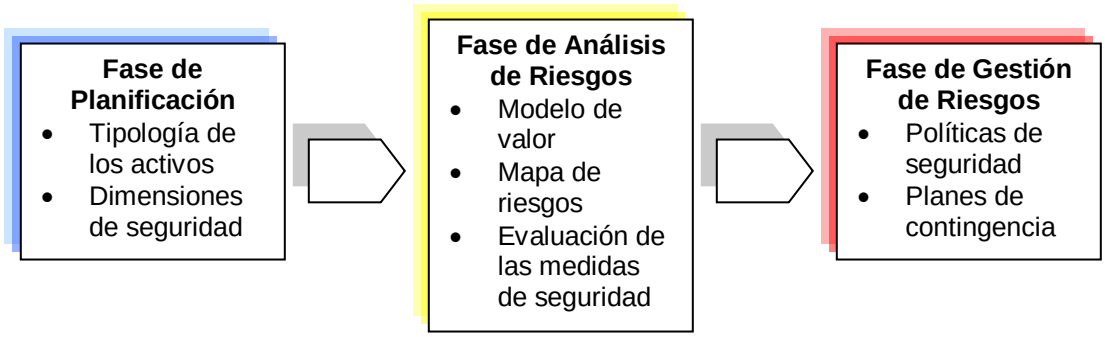


Figura 2. 8 Informes

2.6 Análisis inicial para recolección de información

En esta primera etapa es importante definir y determinar los aspectos más importantes que hacen parte del lugar donde se va a realizar la auditoria, es decir definir una serie de parámetros o encuestas que permitirán determinar las características más importantes y relevantes del lugar de estudio.

En primera instancia es conveniente ubicarse en el estado de la seguridad la manera como se maneja actualmente la información y el grado de conciencia de los usuarios, es por esto que resulta conveniente en primera instancia basarse en cuestionarios y preguntas. Los cuestionarios deben ser atendidos y resueltos por los administradores o por el personal encargado de manera directa de la administración de la seguridad de la información. Estos cuestionarios tratan temáticas que se explican a continuación.

2.6.1 Alcance

Determina las características iniciales y los límites del proyecto, los objetivos y el ámbito que abarcara el proyecto, así mismo las posibles restricciones que se pueden tener y los posibles resultados que se espera entregar, sin olvidar los recursos y los requerimientos puntuales para el desarrollo del mismo. Es importante conocer las características del negocio y el estado actual.

2.6.2 Políticas de seguridad de la información

En esta área es importante determinar si se tiene actualmente políticas de seguridad establecidas, es decir si están formalmente establecidas en un documento, además de tenerse si estas políticas de seguridad son conocidas y puestas en práctica por las personas que se encargan de la administración de la información y los servicios. En caso de que se tengan es importante determinar que tan actualizadas se encuentran con respecto a las nuevas aplicaciones o las necesidad de seguridad que se tiene actualmente y algo muy importante determinar si dichas políticas se encuentran actualmente en funcionamiento, de esta parte surgen resultados importantes, no solo es importante tenerlas definidas, es muy importante hacerlas publicas y emplear los mecanismos para que sean conocidas y usadas tanto por los administradores como por los usuarios, ya que el uso de estas se retribuirá en

un mejor desempeño para la organización.

2.6.3 Organización de la seguridad

Se trata de definir y recolectar información de temas puntuales para determinar si se tiene personal encargado exclusivamente de ofrecer seguridad de la información, es importante determinar si el personal está capacitado para desempeñar este cargo, si se están empleando mecanismos que permiten que este grupo de trabajo se mantenga actualizado y se capacite en esta área específica con asesorías externas, que se trabaje en conjunto con empresas dedicadas a la seguridad de la información. Además es importante determinar si se cuentan con mecanismos adicionales que permiten ofrecer un nivel de seguridad adecuado.

2.6.4 Control y clasificación de activos

Es importante en esta área definir aspectos como: el conocimiento de los activos, si el concepto de activo que se maneja permite clasificar y determinar con claridad la importancia de los mismos y el tratamiento que se le deben dar, los mecanismos se tienen implementados para garantizar la importancia de estos activos y aspectos relevantes a la responsabilidad de la gestión de estos, así mismo si estos activos al estar definidos los demás usuarios son conscientes y responsables por la integridad de estos activos.

2.6.5 Seguridad del personal

Determinar si cuentan con puestos de trabajo definidos, para determinar si el personal realiza labores específicas o todos realizan las mismas labores, así mismo que responsabilidades de seguridad se tienen definidas y asignadas de manera clara y efectiva. Es importante determinar aspectos del personal como: si cuentan con apoyo por parte de la administración para continuar con su capacitación en seguridad de la información, confiabilidad con respecto a los administradores, referencias claras y verificables, es importante determinar si se tienen personal o personas que se han contratado de manera secundaria la cual pudiera influir en la administración de la información.

2.6.6 Seguridad física y ambiental

Importante determinar si se tienen mecanismos o medidas de seguridad para garantizar que el Centro de Datos cuente con mecanismos de seguridad que restrinjan el perímetro y el acceso a los lugares donde se tiene equipos y se maneja información de gran importancia, así mismo se debe determinar si se cuenta con mecanismos de seguridad para que actúen en situaciones inesperadas como fallos de energía e imprevistos afines, es importante determinar qué tipo de acceso se tiene y cual se podría implementar para solventar estos inconvenientes, por otro lado es conveniente tener claro que tan expuestos se hallan los puesto de trabajo a posibles ataques y accesos no permitidos y por último que mecanismos se emplean para mantener actualizado el inventario de equipos y la disponibilidad actual de los mismos.

2.6.7 Tecnologías de la información operaciones y comunicaciones

Se pueden determinar características como: que estándares mantiene o sigue la empresa para el manejo de la información, si tienen planeado la implementación o puesta en marcha de algún estándar para ingresar a un proceso de certificación. Qué mecanismos se tienen para actuar frente a posibles cambios en cuanto a estructura o tecnología, es importante tener en cuenta en esta área los mecanismos que se tienen para la planificación y estudio del software que se va a implementar o las mejoras que se le puede dar al mismo, así mismo un punto que cobra gran importancia y que es un fundamento para dar continuidad y apoyo a las actividades de planificación para hacer frente a situaciones inesperadas, es el sistema de copias de seguridad el cual va a permitir en un momento dado restaurar la información sin que se sufra daño.

2.6.8 Control de accesos

Determinar el control de acceso que se realiza a las instalaciones físicas y a los mismos equipos que soportan la información, para esto tener en cuenta aspectos como: determinar el acceso a los equipos, las restricciones, tipos de privilegios, los distintos usuarios que hacen uso de estos sistemas, las herramientas que permitan realizar un control de los acceso de tal manera que en un momento dado el administrador pueda determinar quien se encuentra en los equipos, que políticas para administración de contraseñas se tienen, es

importante determinar si se tienen mecanismos para asignación de usuarios o si se mantienen mecanismos para administrarlos como por ejemplo caducidad y verificación del nombre de usuario, así mismo determinar los métodos de seguridad que se tiene para acceder a la red y los mecanismos que se emplean para evitar la conexión anónima de equipos a la red.

2.6.9 Mantenimiento y desarrollo de sistemas

Si se desarrollan sistemas es importante determinar la metodología y los métodos que se emplean para el diseño de este software y los mecanismos de prueba para la implementación, se debe determinar qué tipo de seguimiento se le realiza después de la implementación, si se están manejando procesos de documentación que permitan mantener actualizado las fases de desarrollo y pruebas, así mismos que tipos de herramientas se emplean para poder gestionar los equipos y el mismo software que permita realizar análisis de posibles situaciones de riesgo.

2.6.10 Planes de continuidad del negocio

Determinar si se cuenta con planes de continuidad del negocio de tal manera que permita que los servicios puedan continuar con la prestación de los servicios y la manera como se está llevando a cabo, si se tiene es importante conocer si los empleados son conscientes de este plan de continuidad y que políticas tienen para la activación del mismo.

2.6.11 Control de adecuación a las leyes

Es importante saber si se cuenta con herramientas o mecanismos que permitan verificar el cumplimiento de la legislación y de los estándares. Así mismo verificar si se complementan con auditorías externas que permitan verificar el cumplimiento de estos mecanismos, dentro de esto es importante conocer si los empleados son conscientes de los perjuicios y las consecuencias que acarrea el no cumplimiento de las normas.

3 Anexo cuestionario para la recolección de información en el Centro de Datos

Para la recolección de información se organizó un temario con una lista de puntos y factores críticos en los cuales se pueden dar las principales necesidades del Centro de Datos de la Universidad del Cauca, estos temas recogen información de:

3.1 Preguntas para los administradores

3.1.1 Instalaciones físicas

1. El centro datos cuenta con instalación físicas exclusivamente para alojar servidores y equipos de red?.
2. Las instalación cuenta con suministro de aire acondicionado?
3. Se cuenta con sistemas de alimentación de respaldo que permitan mantener el funcionamiento los servidores cuando se tenga un fallo energía. UPS, planta?
4. Se cuenta con doble circuito alimentación?.
5. Dicho centro provee las condiciones necesarias para administrar los equipos?

3.1.2 Conexiones y tipo de tecnología empleada para infraestructura de red

1. Qué tipo de tecnología se emplea para el acceso al medio?
2. Tipo de cableado empleado en la infraestructura de red?
3. Se manejan conexiones inalámbricas?
4. Que topología de red se tiene?
5. Se encuentra certificados los puntos de acceso y conectores?

3.1.3 Equipos de red con los que cuenta el Centro de Datos

1. Se tienen Enrutadores?
2. Se tiene Firewall?
3. Se tienen administradores de ancho de banda?
4. Se tienen Hubs?
5. Se tienen Switchs?
6. Que otros equipos de red se tienen?

3.1.4 Equipos informáticos (servidores) con los que cuenta el Centro de Datos

1. Equipos que se tienen?
2. Qué sistema operativo manejan?
3. Características físicas de los servidores?

3.1.5 Proveedores de ancho de banda

1. Cuántos proveedores de acceso Internet tiene la Universidad?
2. Cuál es la capacidad de sus enlaces?
3. Como es distribuido el tráfico en estos enlaces?
4. Se tiene algún mecanismo para balanceo de carga?

3.1.6 Servicios que actualmente soporta el Centro de Datos

1. Qué tipo de servicios está en capacidad de soportar el Centro de Datos?
2. Que servicios se soportan en el Centro de Datos?
3. Qué servicios adicionales tienen instalados los servidores?
4. Se emplean servicios para gestión de los servicios prestados?
5. Tienen servicios de prueba?

3.1.7 Servicios que presta el Centro de Datos a la comunidad universitaria

1. Que servicios presta?
2. Cuáles son las características de los servicios?
3. Que servicios son más críticos?
4. Que servicios cuentan con mayor uso?
5. Cuáles de estos servicios se encuentran catalogados por su importancia?

3.1.8 Administración, instalación y mantenimiento de los equipos

1. Quién realiza la instalación y mantenimiento de los equipos?
2. Existe algún mecanismo para realizar este proceso?
3. Quien administra los equipos?
4. Se emplea algún tipo de autenticación?
5. El acceso físico a estos equipos es restringido?

3.1.9 Administración instalación y mantenimiento de los servicios

1. Quién instala el software necesario en los equipos?
2. Tienen una política para instalación de software?
3. Quién administra las aplicaciones?
4. Cómo se realiza el mantenimiento de las aplicaciones?
5. Los usuarios pueden hacer modificaciones a las aplicaciones?
6. Quién administra los servicios?
7. Se requiere algún tipo de autenticación para acceder a los servicios?

3.1.10 Estaciones de trabajo

1. Tienen estaciones de trabajo para los administradores?
2. Características en estas estaciones?
3. Manejan algún tipo autenticación?

3.1.11 Características de acceso a los servidores y servicios

1.	El acceso los servidores es restringido?
2.	Qué mecanismos de autenticación se emplean?
3.	Qué mecanismo de seguridad se emplea?
4.	Cómo se asignan los usuarios?
5.	Cómo se asignan las contraseñas?
6.	Se mantiene algún mecanismo de control por la asignación de contraseñas?
7.	Qué servicios requieren un tipo autenticación?
8.	Qué servicios requieren autenticación y cuáles no?
9.	Las aplicaciones pueden ser manipuladas por algún usuario?

3.1.12 Administración de usuarios

1.	Cómo se administran los usuarios?
2.	Se tiene algún repositorio o base de datos donde se encuentran almacenados?
3.	Cómo se puede ser un usuario de la Universidad del Cauca?
4.	Aplicaciones para administrar usuarios?
5.	Tienen usuarios con privilegios?
6.	Cómo se asignan los privilegios a dichos usuarios?
7.	Características de los usuarios con privilegios?

3.1.13 Planes de contingencia

1.	Se tiene planes de contingencia?
2.	Se aplican dichos planes?
3.	Los servidores críticos actualmente tiene algún sistema de contingencia?
4.	El plan de contingencia es actual?

3.1.14 Planes para realizar copias de seguridad

1.	Se realizan copias de seguridad?
2.	De qué se realizan copias de seguridad?
3.	Con qué frecuencia se realizan las copias de seguridad?
4.	Los usuarios pueden acceder a las copias de seguridad?
5.	Las copias de seguridad se encuentran en una ubicación diferente?

3.1.15 Planes de seguridad

1.	Se maneja algún plan de seguridad?
2.	Actualmente existen mecanismos de seguridad?
3.	Quien administra los mecanismos de seguridad?
4.	La seguridad es actual?
5.	Los planes de seguridad contemplan tanto servicios como equipos servidores?
6.	Se maneja el tema de seguridad en cuanto a comunicaciones y conexiones seguras para hacer transacciones?

3.1.16 Información acerca del personal

1. Cuántos administran el Centro de Datos?
2. Cuáles son los estudios de los administradores?
3. Cuál es su turno laboral?
4. Tienen experiencia en seguridad?
5. Han sido capacitados por la universidad?

3.1.17 Funciones del área

1. Cuáles son las funciones principales del área?.
2. Cómo seguir las funciones?
3. Que funciones adicionales realiza el personal del área?

3.1.18 Planes de continuidad

1. Se tienen planes de continuidad y mejora en el Centro de Datos?
2. Estos planes se enmarcan dentro del plan de de desarrollo?
3. Quien dirige éste plan?

3.1.19 Agentes y proveedores externos

1. Hay vinculado personal externo a la universidad?
2. Se tiene algún tipo de prueba, alguna aplicación?
3. Se contrata algún servicio externo para prestación de los servicios?

3.1.20 Historial de amenazas y fallos de seguridad

1. Se emplean herramientas para detección de este tipo de riesgos?
2. Se cuenta con registros de amenazas que han afectado el Centro de Datos?
3. Se cuenta con un registro de riesgos materializados en el Centro de Datos?
4. Se tienen registros del impacto que dichos riesgos hayan generado?

3.2 Preguntas para los usuarios

3.2.1 Cómo perciben la prestación de los servicios

1. Cómo calificaría los servicios prestados?
2. Está conforme con los servicios prestados por el Centro de Datos?
3. Los servicios que presta el Centro de Datos son suficientes?
4. Requiere servicios adicionales?

3.2.2 Cómo perciben la seguridad de la información

1. Ha tratado de violentar o comprometerla sobre el Centro de Datos?
2. Ha logrado explotar algún fallo de seguridad?
3. Ha presenciado fallos de seguridad?
4. Los fallos de seguridad afectan la integridad de la información?
5. Cómo calificaría el nivel de seguridad?

3.2.3 Normas de seguridad que se deben cumplir

1. Conoce las políticas de seguridad y normas que se deben cumplir?
2. Cumple dichas políticas?
3. Ha presenciado el cumplimiento de estas políticas de seguridad?

4 Guía metodológica que permite definir los criterios para establecer políticas de seguridad de la información para un centro de datos de una institución de carácter educativo

4.1 Presentación

La presente guía ha sido elaborada con base en el estudio de normas relacionadas con el tema de gestión de la seguridad de la información, especialmente las normas ISO 17799 e ISO 27001 y el aporte de los autores gracias a la experiencia obtenida como trabajadores del Centro de Datos de la Universidad del Cauca, experiencia que aporta al enfoque de la guía el cual es crear políticas de seguridad de la información que sean de gran utilidad para los entornos educativos a los cuales los centros de datos brindan sus servicios. Los objetivos principales de esta guía son:

- Ser una herramienta que facilite la elaboración de políticas de seguridad de la información para centros de datos en entornos educativos.
- Brindar las pautas y recomendaciones necesarias para la elaboración de las políticas de seguridad de la información.
- Establecer una secuencia que permita de una manera integral considerar todos los puntos relevantes para la creación de políticas de seguridad de la información.

La guía es un planteamiento inicial, no obliga en si al desarrollo completo de ella, por lo que es pertinente aclarar que todo los ítems y demás elementos estipulados conforman una sugerencia y es potestad de quien haga uso de la guía definir cuáles son importantes y necesarios para el desarrollo de su propio proyecto.

La guía se compone de cuatro fases durante las cuales se van dando los criterios a ser tenidos en cuenta para la creación de políticas de seguridad de la información, complementario a esto se encuentra un anexo en el que se dan los criterios para la realización de un análisis de riesgos, lo cual se incluye debido a la importancia que tiene este proceso para una óptima creación de las políticas de seguridad de la información, que

precisamente cubran las falencias que se encuentren en dicho análisis, según lo planteado en la descripción de la fase de inicio.

4.2 Introducción

En la actualidad la prestación de los servicios en los centros de datos de las instituciones educativas son de vital importancia para su desempeño en sus respectivos entornos, la dependencia que tienen estas instituciones de todos los servicios que brindan para el desempeño de sus funciones críticas tanto de la parte administrativa como de la académica, conlleva a pensar muy fuertemente en la seguridad informática, la cual ha alcanzado gran consideración debido a los continuos cambios y amenazas que surgen con el desarrollo de tecnologías, plataformas de computación, la interconexión mundial de redes, amenazas que pueden afectar la prestación de todos los servicios y por ende a toda la comunidad educativa en general.

Por lo tanto, esto lleva al desarrollo de directrices para el uso adecuado de las tecnologías y recomendaciones para obtener el máximo beneficio de ellas, así como evitar su mala utilización, ante esto las políticas de seguridad se dan como una herramienta de tipo organizacional para contribuir en esta problemática y lograr concienciar sobre la importancia, sensibilidad de la información y de los servicios críticos para la institución educativa mantenerse como pionera en su campo de acción.

4.3 Fases para la creación de las políticas para seguridad de la información

Para llevar a cabo el diseño de políticas de seguridad de la información para centros de datos en instituciones educativas, se han establecido una serie de criterios que abarcan todo lo referente a este aspecto, que guían su creación y se han establecido de manera secuencial lo que hace óptimo dicho trabajo. El desarrollo se ha dividido en cuatro fases que consideran cada una dentro de sí mismas las etapas a seguir y puntos a tener en cuenta, fases que se observan en la figura 4.1:

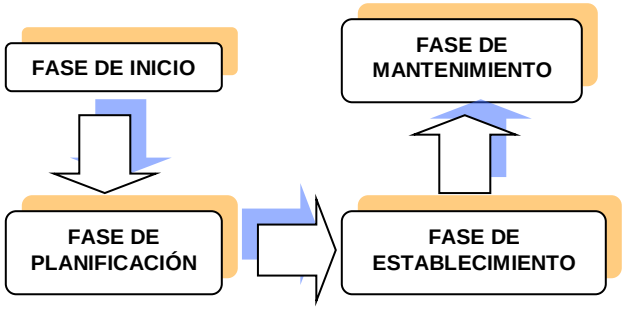


Figura 4. 1 Fases creación de políticas

La primera fase denominada de inicio corresponde a todos los elementos necesarios para iniciar el proyecto como lo son la conformación del equipo de trabajo, la preparación y formación de este equipo en la temática relacionada con la gestión de la seguridad de la información, especialmente en los apartes destinados a las políticas de seguridad. Un proceso muy importante en esta fase es el análisis de riesgos que permite definir un dominio, estudiar la viabilidad y determinar la oportunidad de realizar el proyecto. La segunda fase considerada como la de planeación contiene criterios importantes y bases que llevan a contemplar aspectos que perfilan la fase siguiente para la elaboración de las políticas. La tercera fase denominada de establecimiento contempla las áreas de seguridad de ISO 17799 y otros criterios necesarios para la creación de políticas de seguridad de la información que puedan cumplir con una adecuada gestión de seguridad de la información. La cuarta fase de mantenimiento brinda las pautas para lograr que las políticas de seguridad perduren en el tiempo, adecuándose a los cambios que vayan surgiendo en la institución.

4.3.1 FASE I. Inicio

Objetivo: A través de una serie de etapas consolidar una base fuerte sobre la que se sostendrá todo el desarrollo que se realice en torno a la creación de las políticas de seguridad de la información.

Entradas requeridas: ninguna.

Resultados:

- Documento en el que se informe sobre la conformación del grupo de trabajo, con sus diferentes roles y responsabilidades.
- Documento donde se consigne una aproximación del grado de conocimiento que

tiene el equipo de trabajo sobre la parte teórica de políticas de seguridad de la información. Resultado de evaluaciones.

- Documento con el análisis de riesgos, vital para la realización de las políticas de seguridad de la información.

En esta primera fase considerada como de inicio en la elaboración de políticas de seguridad, se considera necesario tener presentes las siguientes etapas de referencia que esta guía establece para lograr el objetivo y el resultado de esta fase:

1. **Conformación de un equipo de trabajo:** debido a la complejidad y alcance que pueden incluir las políticas, se hace adecuado conformar un grupo de trabajo para su diseño, grupo que debe incluir al personal que se relacione directamente con el centro de datos en cuestión, un representante de la parte administrativa, así como un experto en lo referente a seguridad de la información que puede hacer las veces de asesor y el representante legal de la institución. Los roles que deben asumir son los expresados en la tabla 4.1:

Tabla 4. 1 Roles equipo de trabajo

Rol	Descripción
Coordinador	Puede ser la persona que maneje directamente las redes, sistemas y telecomunicaciones de la empresa, en caso de que este trabajo dentro de la institución sea desempeñado por varias personas, se debe escoger la más capacitada e informada sobre el área en particular para la cual se van a establecer las políticas, o también es factible la selección de una persona con los conocimientos necesarios del tema y con habilidades de administración. Su función principal como su nombre lo dice, es la de coordinar el equipo de trabajo, plantear su visión, misión, alcance, objetivos y demás particularidades que enmarquen el trabajo a realizar, encargado de citar a las reuniones, de velar por el flujo de trabajo adecuado, así como plantear todo tipo de revisiones y evaluaciones que se vayan considerando durante el desarrollo del proyecto.
Diseñador 1 **Diseñador 2**	Un rol lo asumirá una persona representante de las áreas involucradas, con los conocimientos necesarios de la temática, en lo referente a seguridad informática, redes, telecomunicaciones o del campo en particular que sea necesario. El otro será el representante de la parte administrativa, quien deberá ir dando su aval a cada una de las políticas. Sus funciones principales en conjunto son las de crear las políticas de seguridad como tal, ir generando la serie de borradores para que vayan siendo corregidos por los evaluadores hasta obtener el documento final que contenga las políticas de seguridad de la información.
Evaluador 1, **Evaluador 2**	Uno de los evaluadores debe ser el representante legal de la institución, cuya misión es velar por que las políticas que se establezcan cumplan y sobre todo, no violen reglamentos internos así como demás leyes de tipo constitucional y demás de la nación. El otro evaluador, quien puede ser cualquiera de las personas representantes de las áreas involucradas, también tiene como función dar su visto bueno a cada una de las políticas planteadas, revisando su viabilidad, conveniencia, factibilidad, impacto y demás aspectos que se puedan considerar pertinentes.
Asesor	Su función como experto en todo lo referente al campo de seguridad de la información es la de velar porque todo el desarrollo del trabajo este bien enmarcado, ir dando las pautas para su evolución, dar el visto bueno a cada paso que se da, tarea que se establece o responsabilidad que se asigne. Al inicio del proyecto una de sus funciones principales es la de contribuir en la capacitación del equipo de trabajo en la materia de seguridad, velando porque se logre un nivel

	aceptable de conocimientos en el tema y de comprensión total sobre el trabajo que se debe realizar.

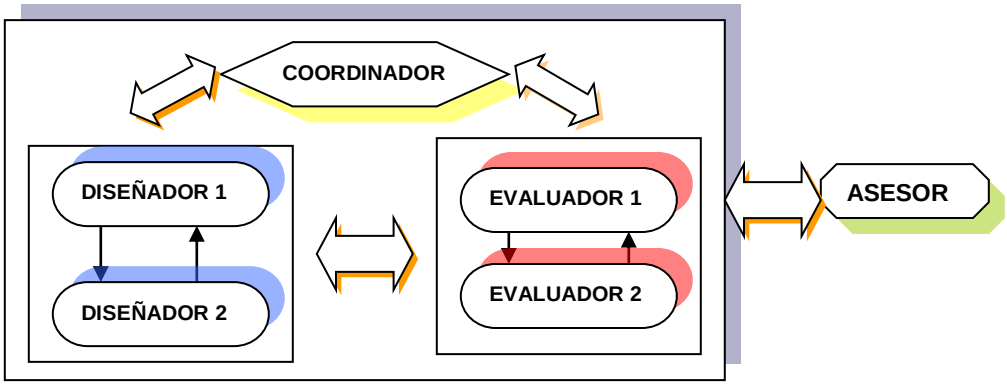


Figura 4. 2 Equipo de trabajo

La figura 4.2 muestra la interrelación de los integrantes del equipo de trabajo.

2. **Conocimiento teórico sobre políticas de seguridad:** antes de introducirse en la elaboración de políticas de seguridad es un aspecto importante el conocer exactamente a qué se hace referencia cuando se maneja el término política de seguridad, cuáles son sus componentes, las clases de políticas de seguridad que se pueden crear, así como la importancia de su establecimiento, para afianzar estos conceptos teóricos se puede tomar como referente el capitulo uno del presente trabajo de grado. Sin este punto al iniciar un trabajo de diseño de políticas, este se podría tornar tedioso y poco efectivo, ya que se puede tender a confusiones, errónea redacción de las normas y demás falencias que se pueden presentar. Para la evacuación de este punto se pueden plantear jornadas de capacitación, en forma de talleres, seminarios y demás, cuyo fruto se debe reflejar en evaluaciones que muestren por parte de cada uno de los miembros del equipo su correcta adquisición de los conceptos, ideas e incluso en lo posible desarrollo de habilidades para la creación de las políticas que se hayan enseñado, pueden ser evaluaciones con preguntas específicas de conceptos, selección múltiple, o la forma que se considere más apropiada de acuerdo a la dinámica del equipo de trabajo.

3. **Realización de un análisis de riesgos:** este es un proceso vital para la creación de políticas de seguridad de la información, la realización de un análisis de riesgos como su nombre lo indica permite la clasificación y control de activos, detectar y valorar todos los riesgos que amenazan la estabilidad y seguridad en las organizaciones, a partir de lo cual se pueden establecer las políticas de una manera más acertada y optimizada.

En resumen el proceso de análisis de riesgo de una manera global se puede definir y expresar como lo muestra la figura 4.3:

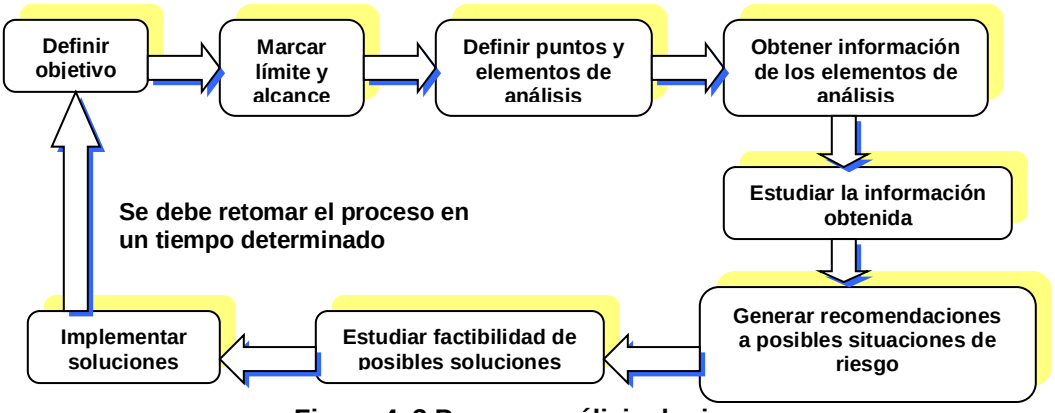


Figura 4. 3 Proceso análisis de riesgos

Para la adecuada realización del análisis de riesgos se debe remitir al anexo de la presente guía metodológica, este contiene los criterios y pasos para realizar el proceso de una manera adecuada. La información y los documentos generados por este proceso son indispensables para continuar con la fase dos de la guía, lo cual se puede ver en la figura 4.4:

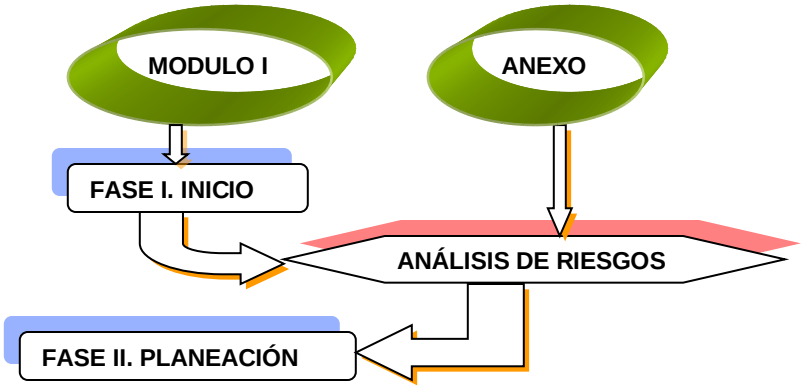


Figura 4. 4 Importancia de un análisis de riesgos

4. Para la elaboración de las políticas, como complemento a lo expuesto anteriormente se pueden considerar aspectos que contribuyen a moldearlas más efectivamente, los cuales se encuentran en la tabla 4.2:

Tabla 4. 2 Criterios para establecer políticas de seguridad

Criterios	Descripción	Recomendaciones
Velar por que las políticas de seguridad tengan las siguientes características. • Que reflejen sus objetivos. • Que contengan una descripción	La definición clara de las políticas de seguridad de la información es indispensable para su entendimiento por parte de todos los involucrados,	• Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y

clara de los elementos involucrados en su definición. • Deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones. • Transmitir por qué son importantes éstos u otros recursos o servicios.	además de pulir su redacción en busca de que se involucren todos los aspectos necesarios para lograr su aplicabilidad.	formalidad dentro de la empresa. • Tener presente que las políticas establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. • Manejo de un lenguaje claro.
Acciones pro-activas.	Tener presente que se debe tender por realizar acciones pro-activas en todo lo referente a la seguridad informática.	• Tomar como base el historial de fallos. • Considerar hasta los riesgos más improbables.
Conciencia de seguridad.	Es de vital importancia para la aplicación de las políticas de seguridad de la información, ya que sin esta su implementación por parte de todo el personal involucrado sería poco efectiva o en el peor de los casos no realizable.	Trabajar en incorporar en todo el personal involucrado la conciencia de seguridad, que no solo se quede en palabras o talleres de capacitación, sino que se logre que cada persona por si misma siempre este pendiente de la seguridad de la información.
Políticas obvias.	Esto contribuye por ejemplo cuando se presentan cambios de personal, lo que es considerado obvio para unos no lo es para otros.	A las políticas de seguridad trazadas no pasar por alto las acciones o hechos que se consideran obvios, todo debe quedar plasmado en un documento.
Tratar la seguridad con independencia y objetividad.	Para establecimiento de las políticas se debe pensar de manera objetiva.	Para esto es importante contar con distintas opiniones.

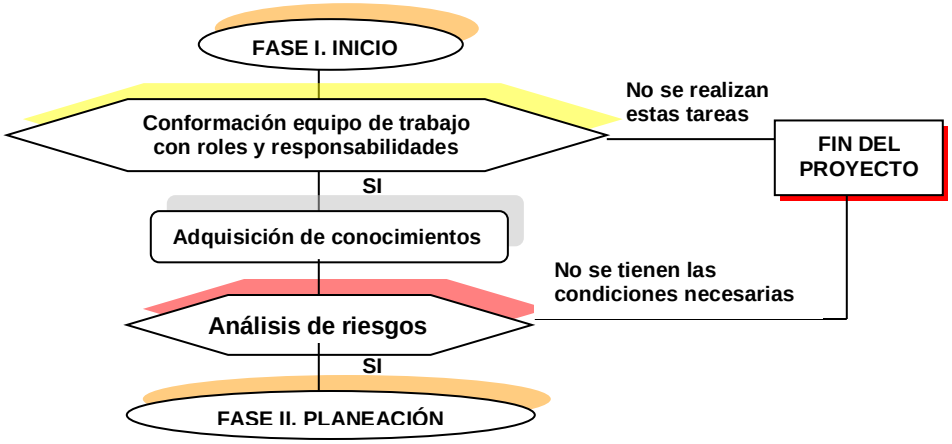


Figura 4. 5 Etapa de inicio

La figura 4.5 muestra el flujo de etapas a seguir y la relación que hay entre ellas, se puede observar que según el resultado de las etapas es posible continuar con la fase posterior o en caso de no lograrlas finalizar el proyecto.

4.3.2 FASE II. Planeación

Objetivo: establecer criterios importantes y bases que llevan a contemplar aspectos que perfilan la elaboración de las políticas.

Entradas requeridas: los resultados de la fase inicial.

Resultado: Documento que recopile el resultado de las etapas realizadas, como lo es que muestre el alcance establecido, el compromiso de la parte administrativa, soportes de las actividades realizadas para el trabajo en equipo, el nivel de seguridad aceptable, listado de las personas que se relacionan con el área, resultado del estudio de las normas. También debe indicar si ya se ha logrado un punto adecuado para iniciar con la fase de establecimiento de las políticas, ya que en caso de no obtenerse se debe retomar desde la revisión de la fase anterior hasta cada una de las actividades que se establezcan en la fase presente. En las tablas 4.3 y 4.4 se encuentran las etapas de referencia a seguir para lograr el objetivo de la presente fase y los criterios que se consideran necesarios:

Tabla 4. 3 Etapas fase de planeación

Etapa	Descripción
Establecer el alcance de políticas.	Es importante establecer el alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Antes de iniciar su elaboración es conveniente establecer este punto, ya que de no hacerlo en el transcurso del trabajo se pueden presentar muchos tópicos que no se han tenido en cuenta y que pueden volver muy extenso y tedioso el trabajo.
Involucrar a toda el área propietaria de los recursos o servicios.	Ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a las políticas de seguridad. Si son muchas las personas que lo conforman entonces deben escogerse dos representantes que conformen el comité de trabajo y los demás pueden ser apoyo en los momentos que se requieran, sobre todo después de que ya se hayan elaborado las políticas, su compromiso debe estar en contribuir fuertemente en su establecimiento y mantenimiento.
Establecimiento de una comunicación eficaz.	Se debe velar por establecer una buena comunicación tanto en el equipo de trabajo para la creación de las políticas, así como con el personal que deba involucrarse. Para lograr este aspecto se pueden realizar talleres de trabajo en equipo que colaboren con el desarrollo de este aspecto.
Establecer las interrelaciones necesarias.	Se deben crear todas las interrelaciones necesarias para el establecimiento de las políticas, su éxito depende en gran medida de que se hayan considerado todas las personas que en un momento u otro intervengan en el proceso. En este aspecto se considera más lo referente a interrelaciones con personas externas a la institución. Para realizar este punto se debe realizar un listado de todas las personas, su tipo de relación, así como una medida de importancia de su participación, su dirección y teléfono de contacto.

Tabla 4. 4 Criterios fase de planeación

Criterio	Descripción	Recomendaciones
Apoyo y compromiso de la parte administrativa.	Es un factor clave el contar con la parte administrativa, ya que es esta la que guía y orienta todo lo relacionado al ambiente institucional, en última es quien da el visto bueno a las acciones que se pretendan tomar.	Para avalar este punto se debe contar con los respectivos documentos firmados que muestren su aceptación y compromiso.
Autoridad en las decisiones.	Recordar que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en proteger los	Dentro de la conformación del equipo de trabajo se debe reflejar este punto dentro de las funciones de sus

	activos críticos de la funcionalidad de su área u organización.	miembros.
Considerar estándares de seguridad de la información.	Basarse en lo estipulado en los diversos estándares relacionados a la seguridad informática, los cuales proveen parámetros establecidos a nivel internacional y brindan orientaciones eficientes para ser consideradas en el trabajo de creación de políticas.	Para este punto se puede obtener la información necesaria en el anexo uno del presente trabajo de grado. Como resultado de este aspecto se puede generar un documento que muestre el estudio que se haya realizado de estas normas, en el cual se aclare que es adecuado y se puede utilizar, o es aplicable de ellas en la institución.
Análisis de requerimientos de seguridad informática.	Consiste en el estudio de la organización, el sistema de información junto a los riesgos para determinar el nivel necesario de seguridad para el adecuado funcionamiento de la organización, este análisis modela las políticas de seguridad que reflejan el estado de seguridad determinado.	El principal resultado de este aspecto es el determinar el nivel de seguridad aceptable, lo cual se puede mostrar determinando unos tres niveles de seguridad, aclarando cada uno a que corresponde o que implica y como cada nivel afecta el funcionamiento de la empresa, se pueden plantear ejemplos para cada nivel.
Aseguramiento de los datos (confidencialidad, integridad, disponibilidad).	Se debe garantizar que la información este siempre disponible, integra y que solo pueda ser accedida por el personal autorizado. Este punto es de vital importancia en la creación de las políticas, debe ser siempre considerado ya que es un objetivo de la gestión de la seguridad de la información.	Lo importante de este aspecto es mantenerlo presente durante toda la realización del proyecto, para que las políticas que se vayan a establecer muestren claramente este aspecto.

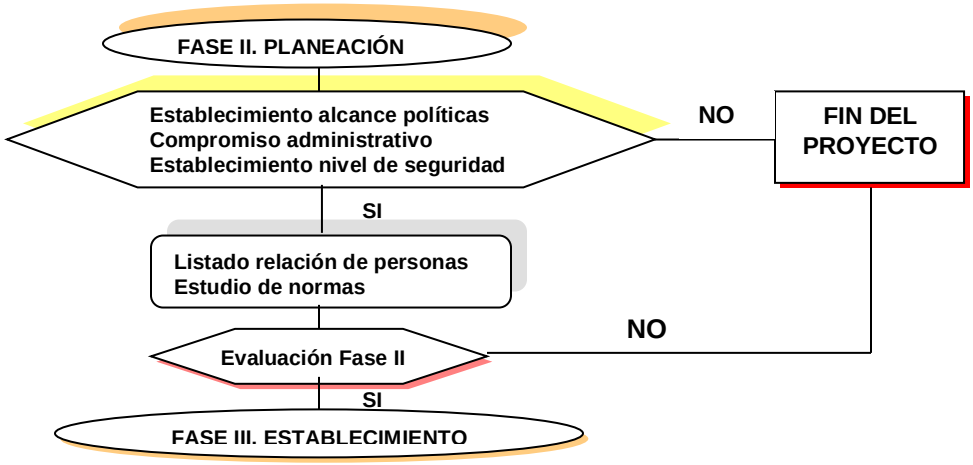


Figura 4. 6 Fase de planeación

En la figura 4.6 se puede observar el flujo de la etapa de planeación, de acuerdo con el resultado de la evaluación es posible continuar con la siguiente fase o en caso contrario finalizar el proyecto.

4.3.3 FASE III. Establecimiento

Objetivo: crear políticas de seguridad de la información tomando como referentes los puntos o dominios principales considerados en la norma de gestión de seguridad de la información ISO 17799.

Entradas requeridas: los resultados de la fase de planeación.

Resultado: Documento con las políticas de seguridad.

La norma ISO 17799 especifica diez dominios o áreas de seguridad, que al hacerlas aplicables en este caso se pueden expresar o determinar en los siguientes criterios de referencia a seguir:

Tabla 4. 5 Criterios con base en las áreas de seguridad de ISO 17799

Criterio	Descripción	Recomendaciones
Política de seguridad.	Donde se deben establecer las políticas de seguridad de la información documentadas, en este aspecto es importante el hecho de que las normas se consideran existentes siempre y cuando se encuentren escritas.	Punto que debe verse reflejado directamente en el documento que contenga las mismas.
Clasificación y control de activos.	Se debe conocer la existencia de todos los activos de la organización que deben ser protegidos.	Punto que se logra plenamente con la realización del análisis de riesgos.
Seguridad organizacional.	Para establecer las correctas bases de la gestión de la seguridad de la información dentro de la organización. Consiste en el establecimiento de procesos que tienen como objetivo mantener un nivel de seguridad adecuado a lo largo del tiempo.	Los procesos no se limitan a procesos de mantenimiento y optimización en el presente, sino que se deben incluir procesos de planeación estratégica de seguridad informática que garanticen que el nivel de calidad se mantendrá en el futuro. Como resultado de este aspecto se pueden obtener planes de revisiones y actualizaciones.
Aseguramiento del componente humano.	Buscar optimizar el componente humano para que su interacción entre los mismos y con terceros sea segura, no filtre información que puede crear vulnerabilidades y que permita detectar ataques de ingeniería social en contra.	Para lograr este aspecto es importante realizar jornadas de capacitación al personal donde se les prevenga de situaciones que pongan en riesgo la información que manejan, jornadas de mesa redonda donde se obtengan todo tipo de sugerencias del personal para lograr mejores comunicaciones, así como detectar fallos y huecos de seguridad que se tengan en este aspecto.
Aseguramiento de la infraestructura física.	Buscar optimizar el entorno físico, que se provean niveles de seguridad industrial adecuados para proteger los componentes del sistema de información que contiene.	Después de realizar un análisis de la infraestructura física, donde se contemplen aspectos que van desde la correcta ubicación de los equipos con sus cables, que se encuentren lejos de zonas de posibles desastres, que cuenten con equipos para monitoreo de entradas y salidas de los equipos de red, hasta la posible utilización de software de monitoreo de red que detecte la perdida de conexiones, que identifique quien y desde qué punto está conectado, etc.

		También se deben evaluar y analizar las medidas correctivas y preventivas del caso que se hagan necesarias.
Control de accesos.	Definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.	Cuando sea factible se deben definir perfiles en niveles de seguridad para el acceso que se autorice tanto a las aplicaciones, equipos y áreas de trabajo, también se deben establecer registros de todos los ingresos y salidas que se hagan.
Continuidad de las operaciones de la organización.	Establecimiento de procedimientos de recuperación en caso de contingencias. Creación de planes continuidad y contingencia que permitan la restauración en caso de contingencias de una manera rápida y que satisfaga niveles de calidad.	Las políticas deben velar y reflejar la búsqueda de la continuidad del objetivo de negocio de la institución. Para este aspecto en la elaboración del plan de contingencia se puede seguir la guía planteada en el capitulo cuatro del presente trabajo de grado.
Aseguramiento de los componentes de ínter conectividad.	Buscar optimizar los componentes de comunicaciones, de manera que los canales funcionen de manera continua y estable, se pueda establecer la identidad de los participantes, que los datos transmitidos sean solo accedidos por las personas autorizadas, que no se puedan modificar los datos y que se pueda establecer el origen de toda comunicación.	Se pueden establecer canales para tener redundancia en caso de fallos, mantener sistemas de autenticación para el acceso a toda la información que lo requiera.
Aseguramiento de los componentes software y hardware.	Buscar la optimización de los sistemas, aplicaciones y componentes hardware, que sean configurados de manera segura y sean utilizados dentro de parámetros de seguridad predefinidos y aceptados, que funcionen de manera continua y estable, con un nivel de calidad aceptable, que no permitan la utilización por personas no autorizadas y que permitan establecer la responsabilidad de uso.	Para la configuración segura de los sistemas y aplicaciones se pueden establecer auditorias de seguridad externas, así como para asegurar el uso autorizado manejar sistemas de autorización, a través de servicios de directorio por ejemplo.
Requerimientos legales.	La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.	Las políticas de seguridad de la información deben concordar con requisitos de tipo jurídico, requerimientos legales e institucionales. Para este aspecto se debe contar con la presencia del representante jurídico de la institución quien tiene como función velar por el cumplimiento de este aspecto.

Como complemento a los anteriores puntos se encuentran las siguientes etapas:

Tabla 4. 6 Etapas de referencia fase de establecimiento

Etapa	Descripción
Definición de violaciones y de las consecuencias del no cumplimiento de la política.	Aunque el fin de las políticas no es el establecer sanciones, si se debe dar a entender en ellas los posibles sucesos de su incumplimiento. Como por ejemplo suspensiones en los servicios, anotaciones a la hoja de vida, memorandos y demás medios que puedan ser considerados.
Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.	Por ejemplo en el caso de todos los dispositivos hardware, estos deben estar bajo la responsabilidad de alguien en particular, por lo general por quien haga uso directo de ellos o este en contacto permanente, lo cual debe verse en documentos firmados donde acepten estas responsabilidades, así como de los servicios de los cuales cada uno es responsable, en este aspecto, en lo posible siempre que se pueda debe existir un solo responsable por cada uno.
Responsabilidades de los usuarios con respecto a la información a la que él o	Cada usuario debe de reconocer la importancia de la información a la cual tiene acceso y firmar cláusulas de confidencialidad.

ella tienen acceso.	
Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.	Contar con los requerimientos estipulados por fábrica, por los proveedores de los sistemas.
Informar a todos los involucrados.	A todo el personal involucrado se le debe informar sobre las políticas de seguridad, se deben plantear mecanismos de difusión para que se logre su establecimiento. Comunicar los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad. Lo cual se puede hacer en jornadas de divulgación.

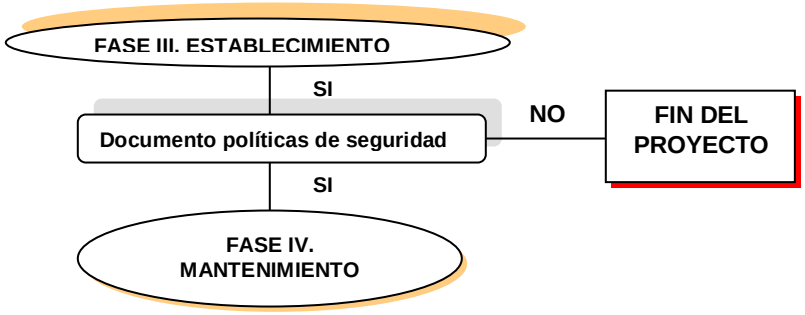


Figura 4. 7 Fase de establecimiento

4.3.4 FASE IV. Mantenimiento

Objetivo: brindar las recomendaciones necesarias para lograr una adecuada utilización de las políticas de seguridad de la información creadas, velando por su mantenimiento y actualización.

Entradas requeridas: los resultados de la fase anterior.

Resultado: Documento con las revisiones, cronogramas de actualización, análisis de reportes de gestión y monitoreo.

Las siguientes son las etapas de referencia a seguir para lograr el objetivo de la presente fase:

Tabla 4. 7 Etapas fase de mantenimiento

Etapa	Descripción
1. Establecer revisiones	Planificación de revisiones continúas a las políticas de seguridad, que pueden ser cambiantes con el tiempo debido a las circunstancias, para garantizar su aplicabilidad. Desarrollar un proceso de monitoreo periódico de las políticas en el hacer de la institución, que permita una actualización oportuna de las mismas.
2. Actualización en la información de seguridad	Mantenerse actualizados de los últimos fallos de seguridad, así como todo lo referente a la seguridad a través de boletines y en la medida de lo posible emitir boletines propios para los usuarios de los servicios.
3. Administración	Establecer políticas de monitoreo de los sistemas estableciendo los

del monitoreo y su reporte	correspondientes reportes. Investigar e implementar herramientas de monitoreo de equipos como Nagios.
4.Establecer un sistema de medición para evaluar el desempeño de las políticas	Se deben planear acciones que utilicen un sistema establecido para saber si las políticas han surtido efecto, lo cual colabora para su actualización y mantenimiento.
5.Establecer procesos de actualización periódica de las políticas sujetas a los cambios organizacionales relevantes	Crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros. Establecer cronogramas con actividades de actualización.

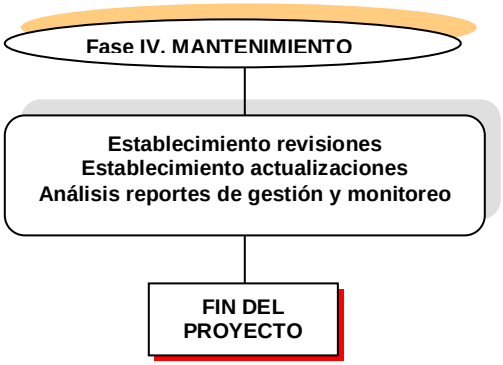


Figura 4. 8 Fase de mantenimiento

4.3.5 CRONOGRAMA DE REFERENCIA 1

Para la realización de las fases de la guía metodológica, un cronograma sugerido es el siguiente:

Tabla 4. 8 Etapas del cronograma de referencia 1

Etapa	Descripción
Fase de Inicio	
1	Conformación del equipo de trabajo.
2	Adquisición de conocimiento teórico sobre políticas de seguridad.
3	Obtención del análisis de riesgos.
Fase de Planeación	
1-2	Definir el alcance y relacionar a todos los involucrados.
3-6	Obtener apoyo administrativo, establecer una comunicación eficaz, reconocer la autoridad en las decisiones, establecer las interrelaciones necesarias.
7	Conocimiento de los estándares de gestión de seguridad de la información.
8-9	Análisis de requerimientos de seguridad y de aseguramiento de datos.
1-10	Con base en los diez dominios de las normas.
Fase de Establecimiento	
1	Establecer responsables.
2	Definir requerimientos mínimos.
3	Información y divulgación de las políticas.
Fase de Mantenimiento	
1	Establecer revisiones

2	Establecer actualizaciones en lo referente a seguridad informática.
3	Determinar administración y monitoreo.
4-5	Evaluar desempeño de las políticas y establecer actualizaciones de ellas.

Etapas	Mes 1				Mes 2				Mes 3				Semana 13			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Fase de Inicio																
Etapa 1																
Etapa 2																
Etapa 3																
Fase de Planeación																
Etapa 1-2																
Etapa 3-6																
Etapa 7																
Etapa 8-9																
Fase de Establecimiento																
Etapa 10																
Etapa 11																
Etapa 12																
Etapa 13																
Fase de Mantenimiento																
Etapa 1																
Etapa 2																
Etapa 3																
Etapa 4-5																

Figura 4. 9 Cronograma de referencia 1

4.4 Anexo criterios para realización de la etapa del análisis de riesgos

4.4.1 Parte I. Análisis y planificación de riesgos

En el establecimiento de los criterios para el desarrollo de un proceso de análisis de riesgos se empleará como referencia la metodología propuesta por Magerit, esta presenta una serie de pasos y recomendaciones basadas en la norma ISO 27001, además una serie de ejemplos y mecanismos que facilitan la realización de los ítems y objetivos propuestos.

Se deben tener claro que en un proceso de análisis de riesgos se cuenta con tres actividades en las cuales se pueden encontrar de manera global puntos que es necesario cubrir. La figura 4.10 presenta algunos de los más relevantes.

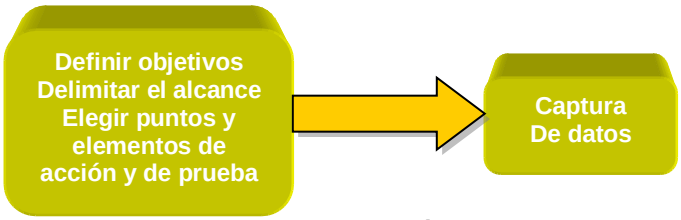


Figura 4. 10 Actividades análisis de riesgos

Planificación: Corresponde a la actividad en la cual se realiza el estudio inicial, se determina la necesidad y la viabilidad del desarrollo del proyecto, se generan y determinan las posibles personas encargadas de llevar a cabo el proceso, así como la manera de solicitar los medios y recursos necesarios. En esta actividad se definen los elementos de partida, el alcance, los límites, los elementos a emplear y el personal necesario para este proceso, también se realiza un proceso de motivación para determinar el grado de necesidad de emplear controles para la seguridad de la información en una institución educativa.

Análisis: En esta parte se define el objetivo general, de acuerdo al estudio previo, donde se establece la necesidad y la viabilidad del proyecto, así como el establecimiento formal de los grupos y comités que harán parte del proceso específico del análisis de riesgos, se establecen roles, funciones, fechas y mecanismos de entrega.

Los roles necesarios para esta parte del proyecto están definidos en la etapa de inicio de la guía metodológica, para estas actividades del análisis de riesgos se requiere del asesor, el director del proyecto y el diseñador o ingeniero quien se encargará de llevar a cabo los procesos y actividades necesarias para la recolección de información.

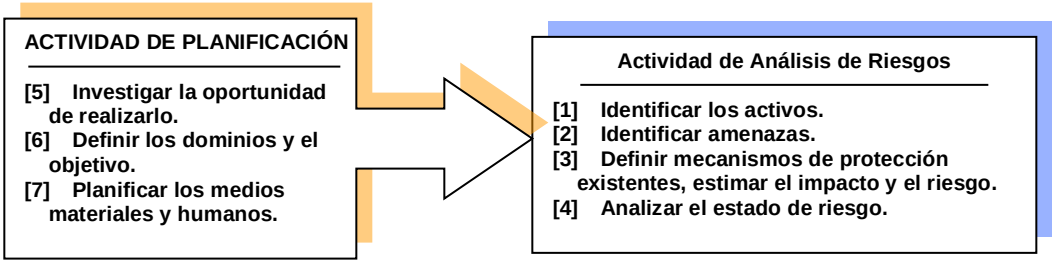


Figura 4. 11 Procesos y actividades

4.4.2 Actividad 1. Planeación

Roles:

Director: Evaluará resultados.
Diseñador: Ingeniero encargado de realizar los procesos.
Asesor: Guiar proceso y evaluar resultados

Resultados:

- Documento con la información referente a la necesidad de seguridad que tenga la institución, así como el grado de aceptación por parte de los empleados.
- Documento con soportes de actividades como charlas. Informe con la motivación inicial para el desarrollo del proyecto.
- Documento que consigne los objetivos del proyecto así como su alcance y el dominio que abarcará, los comités creados, las personas seleccionadas para el desarrollo del proyecto, las actividades y fechas propuestas.

1. Realizar los procesos necesarios que permitan sensibilizar a los empleados y a la administración de la necesidad de la implementación de mecanismos para la protección de la información. Se pueden realizar charlas y conferencias de la importancia de la seguridad, resaltando los beneficios que trae, si es posible se pueden implementar unas pequeñas demostraciones que permitan obtener un mejor resultado.
2. Emplear y generar los mecanismos que puedan determinar y encontrar las necesidades que se tienen en cuanto a seguridad de la información.
3. Desarrollar las actividades necesarias para poder llevar a cabo el proceso, como por ejemplo una reunión donde se puedan definir pautas y capturar la verdadera necesidad de la institución. Se pueden realizar reuniones concertadas, una auditoria programada, se pueden emplear formularios y encuestas para la recolección de información.
4. Para complementar la información obtenida y mirar el nivel de riesgos en el cual se encuentra la institución, se pueden emplear mecanismos que permitan hacer un estudio de tal manera que se obtenga la información necesaria, para esto se pueden emplear métodos de ingeniería social, como por ejemplo correo electrónico, empleo de encuestas y todo tipo de acciones que puedan ayudar a recoger información inicial.

En la tabla 4.9 se encuentran los criterios estipulados para la realización del estudio de la oportunidad:

Tabla 4. 9 Criterios para el estudio de la oportunidad

Criterio	Descripción	Recomendaciones
Estudio de la oportunidad.	Es importante determinar la importancia de la seguridad para una institución, ya que este nivel de seguridad determina la calidad de la prestación de los servicios. Se pueden realizar encuestas y	• Definir el tipo de universidad (publica, privada). • Obtener el número de usuarios.

	trabajos de recolección de información, reclasificar el tipo de información, la manera como se maneja, así mismo se puede recurrir a los empleados para determinar la importancia.	• Numerar los tipos de servicios que ofrecen. • Determinar el número de personas que se tienen para el desarrollo del proyecto.
Información reciente y actualizada.	Recuperar y mantener la información referente al historial de fallos de seguridad y de las posibles amenazas a los que se encuentre expuesto o se haya tenido algún tipo de contacto. Esta parte se puede realizar empleando mecanismos de gestión como herramientas de seguridad tales como detector de intrusos, herramientas de monitoreo y gestión de logs o archivos del sistema de tal manera que se pueda consolidar y obtener información del sistema. Recuperar y mantener la documentación referente a los cambios que se puedan haber presentado en el transcurso de diferentes planes de actualización tanto logísticos como humanos. Estos cambios se pueden actualizar o recuperar de bases de datos, sino se tienen es conveniente manejar herramientas para gestión y administración de recursos.	Elegir entre herramientas de libre distribución, propietarias o gratuitas, para esto tener en cuenta: • Profundidad en el análisis. • Tamaño de los elementos a estudiar. • Costos y presupuesto con el que se cuenta. • Conocimiento y experiencia en el manejo de herramientas. • Fechas de actualización de la documentación. • Emplear estadísticas del uso de servicios y elementos.
Realizar Cuestionarios.	Crear un cuestionario que se adapte a las características de cada negocio de tal manera que al realizarlo se pueda capturar u obtener la mayor información al respecto. Los cuestionarios deben tener información referente a las estadísticas de la institución en aspectos como personas, instalaciones, mecanismos de seguridad, empleados, aspectos de los servicios y características del negocio.	• Conocer el tipo de usuarios (estudiantes, docentes, administrativos, contratistas). • Tener en cuenta los servicios más importantes. • Determinar el uso de los recursos tecnológicos.
Determinar responsables.	Es importante que se definan los responsables de las diferentes unidades organizacionales u operativas que hacen parte del elemento a proteger, así mismo es importante definir las personas que son los responsables de la administración de los servicios y los recursos informáticos. Se debe generar tablas y emplear herramientas para administración de este tipo de información donde se pueda definir que recursos y servicios se tienen, quienes son los responsables de esta administración.	• Que elementos o servicios están a su cargo. • Conocimiento de la temática. • Tipo de información que manejan. • Las labores que realizan. • Tener en cuenta tipos de personas estudiantes, administradores, docentes.
Informar a las unidades afectadas.	Mediante informes escritos y documentos que contemplen la información requerida. Crear un ambiente de conocimiento general de los objetivos, responsables y plazos. Difundir por medios escritos y electrónicos los resultados así como las funciones y valores que se tenían y los plazos que se han determinado para realizar los procesos.	Emplear los medios de comunicación como el correo electrónico, informes escritos, reuniones, circulares. Informar a todas las unidades implicadas el desarrollo del proyecto, su presentación, sus objetivos y la metodología a emplear.
Puntos de Control.	Establecimiento de hitos o puntos de control que permitan ir evaluando los resultados obtenidos. Este establecimiento se puede realizar con el cronograma, los objetivos y actividades planteadas. Los puntos de control también se pueden ir obteniendo conforme se obtienen resultados al igual que la fase anterior se pueden ir ajustando al cronograma.	• Tiempo dimensionado para el desarrollo del proyecto. • Los informes con los resultados propuestos

Generar la documentación.	Generar y permitir el desarrollo de la documentación necesaria para el desarrollo del proyecto, de tal manera que se pueda llevar un informe de todos los resultados obtenidos a lo largo del proyecto. Es importante que se base en las plantillas y ejemplos propuestos en la metodología Magerit si es para un proceso de certificación.	• Debe contener detalles de los puntos más importantes. • Debe ser clara y objetiva. • Debe describir los ambientes estudiados.

Otro aspecto importante es la determinación del alcance del proyecto, para lo cual se establecen los criterios de la tabla 4.10:

Tabla 4. 10 Determinación del alcance del proyecto

Criterio	Descripción	Recomendaciones
Contemplar los planes de actualización.	Tener en cuenta los diferentes planes de actualización que se están aplicando o por los cuales está pasando la organización como por ejemplo, el plan estratégico de sistemas de información o de seguridad general.	• Recopilar información de estadísticas y procesos administrativos. • Trabajar en conjunto con la administración.
Determinar los objetivos según los requerimientos y el tiempo propuesto.	Permite delimitar y enfocar el trabajo hacia la consecución de resultados que están acordes a las necesidades y posibilidades de la institución educativa. Por ejemplo el proyecto puede estar enfocado solo a: • Requerir un estudio de la información y como se ve afectado por la legislación de datos de carácter personal. • Requerir un estudio de las garantías de confidencialidad de la información • Requerir un estudio de la seguridad de las comunicaciones. • Requerir un estudio de la seguridad perimetral • Requerir un estudio de la disponibilidad de los servicios (típicamente porque se busca el desarrollo de un plan de contingencia). • Buscar una homologación o acreditación del sistema o de un producto. • Buscar lanzar un proyecto de métricas de seguridad, debiendo identificar qué puntos interesa controlar y con qué grado de periodicidad y detalle.	• Tipos de servicios. • Tamaño del proyecto. • Costos. • Personal y recursos disponibles.
Determinar las restricciones generales del proyecto.	Dentro de estas se pueden determinar restricciones de tipo: políticas, estratégicas, geográficas, temporales, estructurales, funcionales, legales, relacionadas con el personal, metodológicas, culturales, presupuestarias.	• Presupuesto asignado para el proyecto. • El tiempo propuesto para el desarrollo del proyecto. • Las políticas y necesidades de la institución.
Determinación del dominio y límites.	Determina las unidades que serán objeto del proyecto en cuanto a responsables del proyecto, esta tarea especifica el intercambio de información entre las diferentes unidades que hacen parte del mismo. Dependen de la visión y necesidad del negocio, tal vez no se necesita emplear en aspectos amplios o incluso los recursos con los que se cuenta son limitados, por ejemplo se puede hacer el estudio al centro de datos únicamente en la parte de los servicios.	• Tener en cuenta los objetivos y las restricciones establecidas. • Estudio previo del entorno que será analizado.
Identificación del	Realizar un buen estudio para determinar las	• Definir la dependencia entre las

entorno.	funciones y las relaciones de los entes implicados con el entorno.	diferentes áreas funcionales. • Definir los procesos que se manejan.
Estimación de dimensiones y costos.	De acuerdo a las características y la disposición de la institución, determinando los recursos humanos, técnicos y financieros necesarios para el establecimiento del proyecto.	• El presupuesto económico. • El personal y los recursos con los que se cuenta. • Los tipos de servicios o elementos a estudiar.

Tabla 4. 11 Planificación de los medios materiales y humanos

Criterio	Descripción	Recomendaciones
Evaluar cargas	Permite definir tareas y responsables de las diferentes fases del proyecto. Determinar la carga que el proyecto supone para las unidades afectadas.	• Identificar los puestos de trabajo. • Identificar las áreas importantes en los cuales se debe profundizar.
Planificar entrevistas.	Eso se realiza para tener una visión de las personas encargadas de las áreas a mantener y para tener información precisa de los procesos necesarios.	• Determinar a qué personas se van a entrevistar cuando y con qué objetivo. • Tener en cuenta el conocimiento que tienen del sistema y de la seguridad de la información. • Adaptar los cuestionarios con respecto a las características de cada negocio. • Identificar la información relevante agrupada de acuerdo a la estructura de unidades y roles de los participantes.
Organizar a los trabajadores.	Definiendo las tareas que se han programado en las actividades asimismo tener en cuenta los resultados esperados, este permite determinar quienes participan en la gestión, realización y seguimiento.	Tener en cuenta las habilidades de los involucrados en los procesos, la disponibilidad y conocimiento de la temática
Establecimiento de reglas y modos operativos.	Permite que se establezcan mecanismos de control y seguimiento, así mismo reglas y controles acorde a las metas trazadas en el proyecto.	
Clasificación de la información generada.	Cierta información que es obtenida en el proceso es de carácter privado, por el contenido y la importancia de la mima no puede ser divulgada a todo el personal	• Clasificarla como pública o privada. • Determinar la importancia para el proceso y para la empresa. • Determinar quienes hacen uso de la información.
Planificar el trabajo y establecer un cronograma.	Permite llevar un calendario de las diferentes etapas actividades y tareas del proyecto. El cronograma de actividades permite involucrar a los responsables de las actividades propuestas y los resultados esperados con fechas de entrega que puedan ser verificables y realizables en los tiempos esperados.	• Tener en cuenta los objetivos propuestos, el tiempo estimado para la realización de los procesos y recursos con los que se cuenta. • Establecer las fechas de reuniones, entrega de documentos requeridos, los eventos y resultados esperados. • Definir técnicas y metodologías que se adapten a los procesos y el proyecto para obtener productos.
Criterios de evaluación.	Permiten llevar un control de las actividades y procesos que se están realizando conforme a los objetivos y resultados esperados.	Se deben obtener resultados claros donde se puedan verificar los productos a obtener, así mismo las acciones y elementos para definir

		los datos de entrada y los datos de salida de cada etapa.
Nombrar un promotor.	Es la persona o grupos de personas que se encargan de mostrar la necesidad de la implementación de políticas de seguridad que permitan mejorar el manejo de la información, esta persona puede ser una persona de la misma organización o puede ser una persona externa como un auditor de una empresa encargada para este fin. Igual que el anterior debe ser una persona con suficiente conocimiento del entorno del negocio y la necesidad de la implementación de este tipo de políticas.	• Personal con el que se cuenta. • Estudio de la temática. • Experiencia. • Habilidades en esta temática.

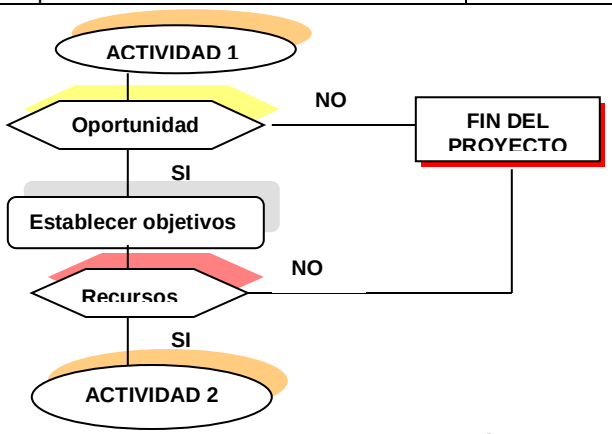


Figura 4. 12 Actividad de planeación

4.4.3 Actividad 2. Análisis

Resultados:

- Informe de activos, amenazas y vulnerabilidades.
- Informe con el estudio de los resultados.
- Informe con la generación de mecanismos para disminuir los riesgos potenciales.

Tabla 4. 12 Actividad de análisis

Criterio	Descripción	Recomendaciones
Se debe identificar los activos.	Permite identificar los elementos importantes para la institución y la valoración que le da a estos.	Emplear herramientas y mecanismos como tablas y formatos para capturar la información requerida. Tener en cuenta los tipos de elementos Determinar los activos de la manera más precisa y completa, identificando su importancia, su descripción y la valoración con respecto a las características de la empresa y desempeño.
Clasificación de la información.	Permite realizar una organización del proyecto y de los elementos importantes que son requeridos en este proceso	Es importante que la recolección de dicha información se realice teniendo en cuenta los diferentes grupos de usuarios que hacen uso de los sistemas, dentro de ellos podemos mencionar los usuarios

		administradores, los usuarios de las aplicaciones, los datos almacenados y los usuarios finales quienes hacen uso estos datos y sistemas. La información se debe seleccionar de las entrevistas de la manera más exacta y completa posible realizando un procedimiento que involucre a los directivos, responsables de los servicios y a los usuarios.
Tipos de activos.	Esta clasificación permite discriminar y generar documentos y tablas en las cuales se consigne ordenadamente los elementos con los que cuenta la institución.	Determinar los tipos de activos, determinando las características y el grupo al que pertenecen, como por ejemplo servicios, datos, equipamientos, las instalaciones físicas e incluso personal.
Establecer y determinar las dimensiones de valoración de los activos.	Con base en la clasificación anterior se realiza un proceso para establecer la importancia de cada elemento.	Determinar de un servicio elementos importantes tales como la autenticidad, la integridad y la disponibilidad.
Establecer y determinar los niveles de valoración de los activos.	Permite asignarle a cada elemento un valor el cual depende del grado de importancia y necesidad que tiene este para el funcionamiento de la institución.	Esta parte se realiza mediante una escala que puede ser establecida por cada institución en la cual se pueda determinar su valor e importancia, por ejemplo se puede determinar una escala de 0 a 10 donde 10 es el valor más alto para los activos.
Identificación de las amenazas		
Identificación y valoración de las amenazas.	Siguiendo un procedimiento similar al de los activos.	Es importante tener en cuenta la experiencia que se ha acumulado a lo largo de diferentes años, de tal manera que se puedan verificar el historial y los registros de situaciones no previstas
Identificación de las medidas de protección		
Identificación y valoración de las medidas de protección existentes.	Permite identificar, clasificar y enumerar todos los mecanismos con los cuales se cuenta para hacer frente a situaciones imprevistas.	Realizando un procedimiento similar al de los activos. Es importante tener en cuenta la formación que han tenido los responsables en seguridad de la información para el desarrollo de los mismos.
Estimación del estado de riesgo		
Estimar el impacto.	Permite asignar una escala de valoración, en la cual se clasifica el daño que se puede sufrir al materializarse una situación anormal.	Para esto se puede emplear una escala determinada por la propia institución y de esta manera lograr una estimación empleando un método cualitativo que permita determinar los niveles de riesgo a los cuales se encuentra expuesta la institución.
Analizar el riesgo y los resultados.	Este permite generar los soportes de información que consignan el estado actual de seguridad y las necesidades que se tiene en materia de seguridad de la información.	Con base en los resultados de los informes se pueden realizar estudios y cálculos que permitan determinar el nivel de riesgo y las características del mismo, con base en esto generar las posibles medidas de protección.

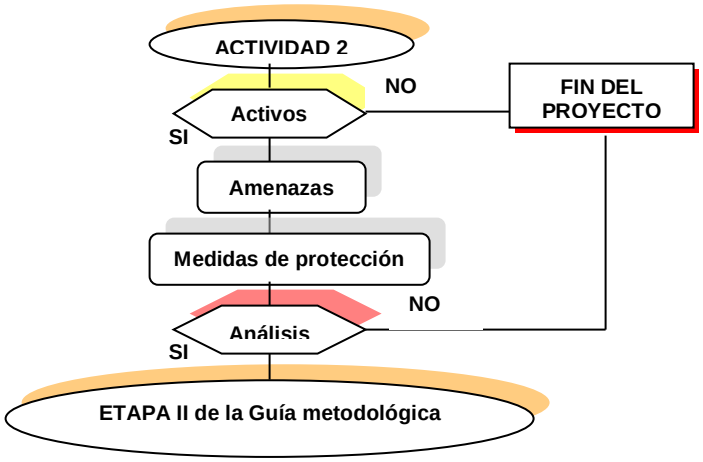


Figura 4. 13 Actividad de análisis

La figura 4.13 muestra los procesos y flujos para esta actividad, asimismo las tareas a seguir según el éxito o fracaso de anteriores actividades. Con el desarrollo de las dos actividades anteriores y la información obtenida se debe retomar la fase II de la guía metodológica para llevar a cabo los procesos correspondientes.

4.4.4 CRONOGRAMA DE REFERENCIA 2

Para el desarrollo de esta primera parte del análisis de riesgos se sugiere seguir un cronograma como el de la figura 4.14 en el que se enmarcan las principales tareas que se deben realizar.

Tabla 4. 13 Tareas Cronograma de referencia parte I

Tareas	Descripción
1	Estudio de la oportunidad
2	Definir los objetivos y el dominio que abarcará
3	Planificar los medios materiales y humanos
4	Identificar los activos
5	Identificar las amenazas
6	Definir los mecanismos de protección existentes
7	Analizar el estado del riesgo

Tareas	Semana 1					Semana 2					Semana 3				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															
3															
4															
5															
6															
7															

Figura 4. 14 Cronograma de referencia tareas parte I

4.4.5 Parte II. Actividad gestión de riesgos

En esta parte se dan las pautas para la realización de los procesos necesarios para analizar e implementar posibles mecanismos de protección de acuerdo a la información obtenida en las actividades anteriores y los mecanismos para la gestión de riesgos, es importante mencionar que se contemplan ciclos que permiten retornar a actividades anteriores de modo que se tengan en cuenta los procesos y cambios que vayan surgiendo en la institución y en el equipo de trabajo.

Resultados:

- Documento con el análisis de posibles mecanismos de protección para la gestión de la seguridad de la información.
- Documento con el análisis de resultados y recomendaciones.
- Informe con el cronograma de posibles actividades de prueba y futuras fechas de revisiones.

Tabla 4. 14 Actividad gestión de riesgos

Criterio	Descripción	Recomendaciones
Determinar la estrategia para mitigar el riesgo		
Analizar los datos obtenidos y la factibilidad de la implementación de mecanismos de seguridad.	Son los mecanismos que puedan hacer frente a las falencias identificadas.	Dependiendo del alcance de estos mecanismos y la relación costo/beneficio establecer los que se puedan implementar de acuerdo a las características de la institución educativa. Analizar las acciones migratorias que se puedan realizar conforme a los mecanismos de protección establecidos y sugeridos.
Generar la documentación y los informes requeridos.	Son elementos que sirven de soporte para la implementación y la solicitud de los recursos necesarios.	La documentación debe ser completa, abarcar todos los ítems del proyecto, debe ser clara y entendible. El informe debe mostrar claramente las estadísticas y los resultados que den soporte a las mejoras presentadas.
Realizar la gestión para la consecución o aprobación de recursos.	Necesarios para lograr la implementación de los mecanismos de seguridad diseñados previamente.	Tener en cuenta las características propias de la institución, como el presupuesto, tamaño, recursos disponibles y objetivos del proyecto.
Determinar los mecanismos de protección oportunos		
Implementar oportunamente las medidas de protección.	Se refiere a las que han sido determinadas como criticas para el funcionamiento de la institución, para lograr prontos y mejores resultados.	Tener en cuenta aspectos técnicos para evitar interrumpir la normal prestación de los servicios. Contar con la debida asesoría y capacitación en el momento de implementar nuevos elementos. Mantener un periodo de pruebas en el que se constate el funcionamiento de las mismas.
Definir la calidad de los mecanismos de protección propuestos		
Recrear escenarios en los cuales se pueda	Esto permite tener una visión de la calidad y	Aunque es una tarea difícil ya que no se puede prever una situación con exactitud, conviene mirar

probar la efectividad de algunas de las medidas de protección propuestas.	efectividad de los elementos diseñados y propuestos para mejorar el nivel de seguridad. Además permite la preparación y programación de pruebas y posteriores revisiones.	que pasaría en el peor de los casos y si al ocurrir dicha circunstancia esta se puede mitigar realmente conforme se necesita. Como por ejemplo determinar si cuando falta la energía se puede recuperar el servicio, es decir los sistemas auxiliares proveen los mecanismos necesarios para que esto se lleve a cabo.

En la figura 4.15 se pueden observar las tareas que se pueden realizar en esta actividad, se observa que la calidad de los mecanismos es un punto fundamental para lograr los objetivos trazados.

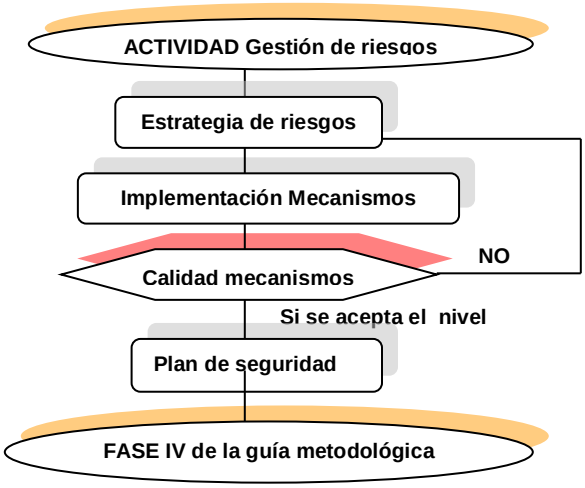


Figura 4. 15 Actividad gestión de riesgos

4.4.6 CRONOGRAMA DE REFERENCIA 3

Para el desarrollo de esta parte se sugiere seguir un cronograma como el de la figura 4.16 en el que se enmarcan las principales tareas que se deben realizar:

Tabla 4. 15 Tareas cronograma de referencia 3

Tarea	Descripción
1	Definir la estrategia para mitigar el riesgo
2	Determinar los mecanismos de protección
3	Determinar la calidad de los mecanismos de protección
4	Diseñar el plan de seguridad

Tarea	Semana 1					Semana 2				
	1	2	3	4	5	6	7	8	9	10
1										
2										
3										
4										

Figura 4. 16 Cronograma de referencia 3

5 Plan de contingencia para el Centro de Datos

Debido a las características y la importancia del Centro de Datos de la Universidad del Cauca, es importante definir el ámbito que abarca dicho plan de contingencia, antes de esto se debe recordar que actualmente existe un proceso de creación de políticas de seguridad, lo que le permite en cierta medida estar preparado para afrontar varias situaciones anormales, por esta razón el plan de contingencia tendrá un enfoque dirigido a la solución de desastres naturales y desastres informáticos.

El presente plan de contingencia se desarrolló teniendo en cuenta los pasos y recomendaciones dadas en el capitulo cuatro del presente trabajo de grado “Criterios y recomendaciones para la generación y diseño del plan de contingencias para el Centro de Datos de la Universidad del Cauca”, por lo tanto se plantea en los siguientes pasos:

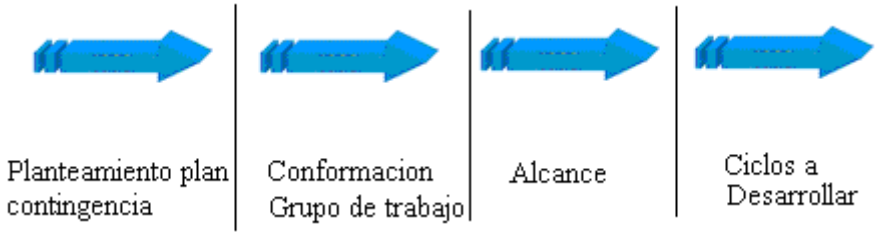


Figura 6. 1 Etapas para la realización del plan de contingencia

1. Definición del planteamiento del plan de contingencia: este se plantea para afrontar desastres informáticos y desastres naturales, se toma este enfoque debido a las necesidades del Centro de Datos y el enfoque dado al presente trabajo de grado, además que estas funciones complementan las fases de análisis y gestión de riesgos previamente realizados.
2. Para la conformación del grupo de trabajo, se tomo en cuenta los roles y la funcionalidad establecidas en el proceso para la creación de las políticas de seguridad:

   Coordinador: Administrador del área de servicios y servidores de Internet de la Red de Datos.
   Diseñador 1: Estudiante del proyecto de grado.

Diseñador 2: Estudiante del proyecto de grado.

Evaluador 1: Administrador del área de servicios y servidores de Internet de la Red de Datos.

Evaluador 2: Jefe división de Sistemas Universidad del Cauca.

Asesor: Docente departamento de Sistemas Universidad del Cauca, con conocimientos en seguridad informática.

3. Alcance del plan de contingencia: será aplicado en lo concerniente a los servidores y equipos importantes que soportan servicios como: el Web, Proxys, Correo electrónico, resolución de nombres, transferencia de archivos por ftp, administrador de ancho de banda, equipos de red internos y externos, así mismo instalaciones y elementos importantes como UPS y sistema de refrigeración los cuales son necesarios para el correcto funcionamiento de los elementos hardware.
4. Ciclos a desarrollar: para esta parte se mantiene y se emplea un paradigma en el cual se debe tener en cuenta aspectos como el antes, durante y después, su uso radica en que permite cubrir los aspectos más importantes para poder llevar a cabo un proceso de contingencia, a continuación se realiza una explicación en cada una de estas tres etapas.

Tabla 6. 1 Etapas del plan de contingencia

Etapa	Descripción
Antes	Corresponde a lo relacionado con la educación, formación, capacitación, difusión y recolección de información y de los elementos más importantes y los planes y medidas realizadas para definir este proceso.
Durante	En esta etapa se realiza todo lo concerniente al estudio del posible problema, puesta en marcha de los elementos definidos y necesarios para garantizar la continuidad de los servicios y sistemas, así mismo la forma como el personal debe actuar frente a dichas situaciones.
Después	Relacionado con la consecución de elementos importantes para cada sustitución, reparación y puesta en marcha de los servicios y equipos tal y como se requiere para retornar los servicios a sus condiciones normales.

El plan de contingencia se aplicará principalmente a la prestación de los servicios más importantes tales como el servicio Web, DNS, correo electrónico, Proxy, FTP y el servicio para realizar copias de seguridad.

5.1 Acciones primarias del plan de contingencia.

Corresponde a las acciones primarias que se deben realizar para afrontar situaciones inesperadas, con el fin de mitigar los posibles daños que se pueden originar.

1. Hay que mantener equipos que puedan denominarse réplicas o equipos de respaldo de los servidores principales. Los equipos de respaldo deben contar con el mismo software y las mínimas características hardware que permitan asumir las funciones de los equipos principales. Se recomienda emplear software Heartbeart que permitirá que dos máquinas trabajen de manera paralela, por lo tanto reciben información actual que permite recuperar el servicio de una manera inmediata, de esta manera se garantiza que cuando deje de funcionar el servidor principal, el secundario tomara esta función. Los equipos que deben contar con réplicas son el Web, DNS y los servidores de correo, servidores de autenticación de usuarios y enrutamiento de correos. Estas replicas deben alojarse en una sede diferente a la principal y debe contar con las mismas características.
2. Dentro de las funciones del personal está el continuo monitoreo en los respectivos turnos de trabajos, por lo que al presentarse un desastre se debe informar en orden de prioridad al administrador de los servicios y a los monitores del Centro de Datos, si hay problemas de infraestructura de redes al ingeniero encargado de la infraestructura de red de la Universidad, si hay fallas eléctricas al ingeniero jefe del área de equipos, si hay fallas de equipos de red se deben comunicar con los respectivos proveedores.
3. Se deben realizar revisiones mensuales a los backups de los archivos principales y de los servidores.
4. El espacio físico secundario que alojará los servidores secundarios, se debe encontrar alejado del centro principal, dicho centro debe contar con las características mínimas de seguridad.
5. Se debe contar con fuentes de protección y elementos diseñados para proteger los equipos cuando fallan los suministros de energía, de tal manera que permitan proteger frente a sobrecargas eléctricas, estos equipos pueden ser reguladores de voltaje o cortapicos. Mantener los debidos repuestos, para sí se sufre un daño grave, se pueda realizar la reposición o el cambio de una manera rápida y efectiva.
6. Se debe velar porque los nuevos equipos de red y servidores que se vayan a adquirir, así como los ya existentes, cuenten con doble fuente de alimentación, de tal manera que se pueda suministrar la potencia desde dos circuitos de alimentación diferentes, dando así la redundancia necesaria para afrontar fallas de energía. Es importante mantener dos circuitos eléctricos con suministro de potencia diferente, de tal manera que permitan tener conectadas las fuentes de los servidores a circuitos

independientes y así aprovechar la redundancia que brindan los equipos con doble fuente. Revisar en la instalación de los servidores que se conectan las fuentes de potencia a circuitos diferentes.

7. Mantener los circuitos de alimentación y de emergencia como las UPS en óptimas condiciones de carga, así mismo verificar que las existentes pueden soportar los equipos que se tienen y la cantidad de potencia que ellos requieren, para de esta manera garantizar la no interrupción del servicio en caso de que falle uno de ellos. Debe revisarse que la autonomía de las UPS sea superior a media hora, de manera que se dé la oportunidad de actuar y reaccionar frente a una falla.
8. Se debe contar con una planta de energía capaz de brindar la potencia necesaria para los equipos y servidores principales, preferiblemente la planta de funcionar con combustible de fácil adquisición.
9. El mecanismo encargado de accionar la planta energía auxiliar debe funcionar de manera automática cuando detecte fallos en el suministro de energía, asimismo debe detenerse de manera automática cuando se restablece el suministro.
10. En las instalaciones donde se ubican los servidores principales así como donde se vayan a ubicar las replicas, se debe revisar y controlar periódicamente el funcionamiento del sistema de enfriamiento, ya que el fallo de este sistema puede ocasionar daños irreversibles en los equipos y servidores.
11. Toda la documentación del área de servidores y servicios de Internet, en especial la referente a servicios, se debe mantener actualizada de manera que se pueda emplear para reparación y reinstalación de los servicios cuando suceden fallos, para de esta manera contar con la documentación necesaria que permite identificar los pasos a seguir para la recuperación de los servicios.
12. Se deben mantener copias de los archivos de configuración recientes, de tal manera que permitan recuperar los servicios y la información de manera rápida.
13. Se debe mantener el software y los paquetes necesarios para recuperar y reinstalar los servicios.
14. Hay que mantener las copias de seguridad de los archivos de configuración y el software necesario para este proceso en el centro principal y en lugares diferentes a las instalaciones principales, tales como el Centro de Datos secundario o un archivo que manejen para guardar información clasificada.
15. Capacitar al personal encargado de la administración de servicios en las acciones necesarios para llevar a cabo estos procesos.

16. Se deben mantener copias de las actualizaciones de seguridad aplicadas a los servidores.

5.2 Plan de contingencia general

5.2.1 Plan de contingencia para la recuperación de servicios

Los servicios esenciales tales como: servicio Web, resolución de nombres, transferencia de archivos, navegación, correo electrónico, autenticación y enrutamiento de correos son servicios que requieren especial cuidado y necesitan ser atendidos de una manera oportuna para que cuando salen de funcionamiento no entorpezcan la funcionalidad del Centro de Datos.

Tabla 6. 2 Recuperación de servicios

Etapa	Descripción
Antes:	• Mantener revisiones semanales de software, buscando posibles deterioros o sobrecargas incluso mal funcionamiento. • Se debe realizar revisiones de los recursos, de la utilización del procesador, de memoria, de discos y periféricos de entrada y salida como las tarjetas de red. • Realizar monitoreo del software y los servicios que se encuentran ejecutando para detectar posibles inconvenientes registrando la información obtenida. • Monitorear aplicaciones y elementos adicionales que permiten que los servicios se ejecuten. • Realizar jornadas de capacitación y difusión de la información y los reportes obtenidos, si en el proceso de análisis se encuentran fallas, estas deben ser comunicadas a los administradores, para que se prevean acciones necesarias para estos posibles fallos.
Durante:	• Si los servicios fallan por el hardware, se debe contar con equipos que permitan funcionar como servidores de respaldo, con la capacidad de soportar la funcionalidad de dicho sistema o servicio. • Si se presenta una situación anormal en la cual falla un servicio esencial, lo primero que se debe realizar es la revisión de los recursos físicos de los cuales hacen uso los servicios, tales como memoria RAM, procesador y espacio en discos. • Si es necesario reiniciar los servicios, se debe tener en cuenta que no pueden haber aplicaciones corriendo o datos en proceso críticos ya que se pueden perder. • Cuando la falla se presenta por los archivos de configuración, estos deben ser reemplazados por archivos de configuración que se tienen en backup y de los cuales se tiene certeza de su funcionamiento. • Si se encuentran aplicaciones desconocidas o procesos que puedan afectar el desempeño de los servicios, dichos procesos deben ser identificados y detenidos manualmente. • Si no es posible restaurar el servicio en el equipo encargado de prestar esta funcionalidad, instalar en un equipo réplica que sea capaz de soportar la funcionalidad básica de los servicios que se encuentran fallando.
Después:	• Evaluar el funcionamiento y desempeño de los recursos debido a problemas con los servicios o aplicaciones debido a situaciones inesperadas. • Reemplazar en el menor tiempo posible el software y los elementos que se encuentran fallando, para este caso verificar si se tiene soporte técnico, si lo tiene contactar al soporte para de esta manera obtener una versión de software estable. Si es necesario instalar software con las actualizaciones o versiones actuales. • Realizar actividades para reinstalación en primer estancia de los servicios, si este procedimiento no se puede llevar a cabo debido a problemas del sistema operativo realizar la reinstalación del mismo, para esto tener en cuenta instalar las versiones y el software

	adecuado y requerido. • Iniciar los servicios y restaurar los datos que involucran usuarios externos y elementos importantes del sistema. • Verificar que los servicios están en correcto funcionamiento. • Verificar la posibilidad de instalar nuevas versiones o actualizaciones de seguridad. • Generar un documento en el cual se consigne la información referente a las fallas que se han presentado y la solución que se le ha dado, asimismo enmarcar la efectividad de los procesos utilizados.

5.2.2 Recuperación del hardware en general

Tabla 6. 3 Recuperación de hardware

Etapa	Descripción Actividades
Antes	• Mantener revisiones periódicas y permanentes de los diferentes equipos con los que se cuenta, de tal manera que se puedan encontrar posibles deterioros o malos usos. • Realizar un inventario en el cual se puede consignar la información de los elementos, discriminándolos por marca y por características técnicas, asimismo determinar si cuentan con la garantía. • Mirar posibles proveedores de acuerdo al presupuesto económico y el presupuesto del Centro de Datos, asimismo tener en cuenta la facilidad y disponibilidad de la consecución de elementos. • Mantener un manual de funcionamiento y configuración de cada elemento hardware.
Durante	• Si fallan los elementos hardware y se presentan problemas por sobrecalentamiento o por usos indebidos, tratar de retornar a las condiciones normales. • Realizar pruebas de conectores y funcionamiento de los elementos. • Remitirse a los manuales de operación y mantenimiento. • Realizar pruebas a los equipos tales como conectividad, ejecución de procesos y uso de recursos físicos. • Si continúa el problema apagar el equipo y con las condiciones adecuadas de seguridad realizar pruebas al hardware.
Después	• Detectar la falla, documentarla y adicionar posibles soluciones. • Realizar un registro de los elementos que fallan. • Contactar a los proveedores para verificar la vigencia de la garantía. • Realizar los respectivos reemplazos de partes hardware, para esto mantener las precauciones necesarias. • Iniciar los sistemas para constatar el funcionamiento y las condiciones de uso.

5.2.3 Recuperación de instalaciones físicas

Tabla 6. 4 Recuperación de instalaciones físicas

Etapas	Descripción de actividades
Antes	• Realizar revisiones periódicas de los elementos e instalaciones físicas, para detectar posibles anomalías tales como humedades, fugas de agua, cortos eléctricos o deterioro de las instalaciones y de la infraestructura. • Mantener un esquema que muestre la ubicación de los elementos con los que se cuenta, marcando las áreas que representan mayor cuidado y las que se encuentran más expuestas a daños. • Programar jornadas de mantenimiento de tal forma que se tenga en correcto estado los elementos y equipos que hacen parte de esta infraestructura.
Durante	• Emplear las herramientas necesarias para mitigar la situación tales como extinguidores, circuitos de protección e interruptores de tal manera que se mitigue el riesgo de aumentar dicha valoración y daño. • Realizar el oportuno aviso a las entidades y organismos competentes para que puedan actuar de una manera oportuna. • Deshabilitar las fuentes de alimentación mientras se tienen las situaciones de emergencia.

	• Salir de las instalaciones y permitir que las personas expertas se encarguen de la solución del problema. • Mantener los equipos y servidores de respaldo en ubicaciones seguras y alejadas de la principal. • Acatar los procedimientos estipulados de tal manera que se puedan realizar las tareas eficientemente.
Después:	• Realizar inventario de daños y de situaciones anormales que afecten el Centro de Datos. • Comunicarse con los proveedores y personas especializadas en este proceso de manera oportuna, obtener cotizaciones de precios para suplir y reemplazar los equipos dañados. • Realizar la reinstalación, configuración de los servicios y recuperación de la información necesaria para restaurar los servicios para garantizar la continuidad. • Poner en funcionamiento el centro secundario para que de esta manera se presten los servicios básicos. • Realizar una bitácora del sistema, donde se consigne información referente a los incidentes presentados y la solución dada a los mismos, para de esta manera definir cómo se puede mejorar el plan de contingencia actual. • Realizar y proponer mejoras que puedan ayudar al desempeño del sistema.

5.2.4 Plan de contingencia para el personal

Tabla 6. 5 Plan de contingencia para el personal

Etapa	Descripción Actividades
Antes	• Realizar capacitaciones previas de cómo se debe actuar frente a situaciones de riesgo que pongan en peligro la integridad física de las personas y de los equipos. • Mantener contactos con organismos que puedan ayudar si se presenta una catástrofe que interrumpa el funcionamiento los servicios
Durante	• Realizar los procedimientos definidos en las normas de seguridad y en la capacitación necesaria. • Emplear manuales y herramientas establecidas para este proceso. • Principalmente buscar la seguridad y los medios que permiten lograr una seguridad adecuada para las personas.
Después	• Realizar actividades de control que puedan brindar las atenciones oportunas. • Emplear mecanismos para recuperación y mejora, de tal manera que se pueda tener un proceso más rápido y eficaz.

5.3 Plan de contingencia para los servicios principales

5.3.1 Servicio Web

La importancia de este servicio es alta debido a que es la cara visible hacia Internet, por tal motivo cuando ocurre un fallo que interrumpe el funcionamiento de este servicio se debe recuperar lo antes posible. Con los documentos previos de análisis de riesgos se puede observar que aplicaciones tiene instalado dichos servidor WEB.

Tabla 6. 6 Plan de contingencia servicio Web

Etapa	Descripción
Antes:	• Generar un documento con los archivos y software necesario para el funcionamiento de éste servicio. • Monitorear el funcionamiento y comportamiento de los servicios. • Mantener una copia de los archivos de configuración tanto para servicio Web como para los servicios suplementarios que contribuyen a este servicio.

	• Mantener una copia de los paquetes y el software necesario para instalar los servicios. • Mantener una copia de seguridad de las bases de datos, sitios Web, llaves y certificados digitales. • Instalar un servidor secundario que pueda asumir la responsabilidad del primario, debe ser una réplica capaz de soportar la funcionalidad básica así como la funcionalidad de servicio Web.
Durante:	• Cuando ocurre una situación terminar los procesos y aplicaciones que están funcionando. Detener los servicios y guardar la información. • Reiniciar los servicios, si no es necesario el equipo como tal. • Detener las conexiones de red y conexiones activas y reiniciar dichas conexiones. • Iniciar mecanismos para detección y control de accesos no permitidos al equipo. • Restaurar la contraseña de administrador, se deben cambiar si han sido comprometidas. • Si la falla persiste, habilitar los servicios requeridos para el portal Web únicamente. • Recuperar los servicios adicionales tales como bases de datos, soporte para aplicaciones como Java y php. • Si es posible habilitar los sitios adicionales que son soportados sobre el Centro de Datos, para sitios que no son de la Universidad, dar un tiempo prudente de espera para habilitarlos. • Cuando se debe instalar el sistema operativo se debe instalar la última versión de sistema operativo estable, con los respectivos parches de seguridad y actualizaciones pertinentes para esta distribución. • Referirse la documentación del área de servicios servidor de Internet para instalar y configurar los servicios tales como: apache, Java, Mysql, Php4, Postgresql, phpmyadmin, rsync, scponly, gcc, pitón. • Restaurar los certificados digitales. • Restaurar información de las bases de datos y el sitio de la Universidad. • Restaurar información con respecto a usuarios y contraseñas del sistema. • Se deben realizar pruebas de los servicios verificando que dichos servicios se encuentren activos, verificando que los procesos esenciales se encuentran en funcionamiento y consumiendo los recursos necesarios, realizar pruebas para verificar que la página de la Universidad es accesible desde la red interna y desde redes externas, verificando también que las aplicaciones que dependen de esta página se encuentren activas.
Después:	• Restaurar el servidor principal. • Analizar los archivos del sistema. • Generar reporte de daños • Reinstalar los servicios si es necesario. • Reinstalar el sistema operativo si es necesario. • Instalar versiones superiores y recientes del software del cual se tiene instalado. • Estudiar la posibilidad de reinstalar nuevo hardware capaz de soportar con mayor eficacia los servicios. • Realizar pruebas para verificar el funcionamiento de apache, apache-ssl. • Verificar la conectividad y el acceso a la página principal. • Verificar el funcionamiento de aplicaciones secundarias como Java, Tomcat, PHP, Mysql, Postgresql, vsftpd. • Verificar es funcionamiento de las aplicaciones soportadas. • Mantener un servidor de réplica capaz de soportar las aplicaciones que son importantes tales como servicio de hosting. • Iniciar e instalar el equipo en un lugar seguro, lejos de peligros que lo puedan afectar.

5.3.2 Recuperación del servicio DNS

Tabla 6. 7 Plan de contingencia del servicio DNS

Etapa	Descripción
Antes:	• Realizar copias permanentes de los archivos de configuración de las zonas que se tienen actualmente configuradas. Esos archivos encuentran en /var/named/ • Realizar copias de la carpeta /etc/bind, donde se encuentran información de la configuración de los servicios. • Mantener copias de los paquetes y el software necesario para instalar las versiones apropiadas.

	• Monitorizar el funcionamiento del sistema para encontrar posibles inconsistencias o fallos. • Realizar un inventario del análisis de los archivos de monitorización para determinar el desempeño y las características de funcionamiento del sistema.
Durante:	• Detener los servicios si es necesario reiniciar o incluso apagar el sistema. • Si es posible verificar que el servicio DNS están funcionando, que el puerto asociado se encuentra en funcionamiento, puerto 53 y que acepte conexiones entrantes y salientes. • Si no es posible iniciar el servicio verificar el error, si es por algún daño en el archivo de configuración restaurar este por uno de respaldo reciente y reiniciar el servicio. • Realizar pruebas con herramientas como dig y nslookup. • Verificar que aplicaciones se encuentran corriendo, y que no interrumpan el funcionamiento del servicio, tratar de eliminar o parar estas aplicaciones. • Si la contraseña se ha visto comprometida cambiarla inmediatamente por una segura. • Cambiar los certificados de los equipos conocidos y las claves de SSH. • Montar una réplica con el archivo de configuración y restablecer los servicios del equipo para que puedan suplir la funcionalidad del equipo principal. • Cuando se necesita recuperar el servicio y el equipo ha fallado en cuanto a hardware o software se debe mirar los procedimientos para el cambio de hardware y software. dentro de los parámetros que se deben mirar son el consumo de procesador, memoria los discos duros, periféricos de entrada y salida así como los elementos de red, este procedimiento se debe realizar de una manera rápida y efectiva. • Si se encuentra un fallo en el hardware realizar el procedimiento estipulado para esto. Si al reemplazar un elemento, el equipo está fallando se debe instalar el servicio en equipo que cumplan las características mínimas para el DNS el cual por sus características no requiere mucho procesamiento y puede ser instalado en las estaciones de trabajo. • Cuando falla el sistema operativo realizar los pasos para restauración de software para este caso instalar la última versión estable del sistema operativo empleado, esta versión debe ser instalada con los respectivos parches de seguridad y actualizaciones del sistema. • Se debe contar con los parámetros en cuanto a discos duros, uso de memoria así mismo parámetros de seguridad mínimos tales como las reglas de seguridad y los usuarios que accedan al sistema. • Para reinstalar el servicio, se instala la última versión de BIND9 o la aplicación para resolución de nombres que se esté usando, en la documentación necesaria del área de servicios de Internet se encuentran información referente a la configuración del servicio. Posteriormente recuperar las copias de seguridad y los archivos de configuración y las zonas de resolución inversa y directa. • Después de realiza los procesos restaurar el sistema y los servicios. • Realizar las pruebas de resolución de nombres con herramientas como nslookup, comprobando la resolución de sitios de la Universidad y de sitios externos, emplear herramientas como Dig para verificar el desempeño y la funcionalidad del servicio. Por último se verificar que los equipos de la Universidad pueden navegar en sitios internos y externos a la red de la Universidad. • Verificar la resolución inversa de zonas con herramientas como DNSstuff para verificar que los sitios pertenecientes a la Universidad se están resolviendo desde sitios externos.
Después:	• Cambiar los elementos software o hardware que se han deteriorado. • Reinstalar el sistema operativo si se necesita. • Restaurar el servicio de DNS. • Recuperar los archivos de configuración. • Probar el funcionamiento de los puertos si es necesario. • Generar un documento con reporte de daños y con la causa de los daños, documentar el proceso realizado.

5.3.3 Recuperación del servicio de correo electrónico

Tabla 6. 8 Plan de contingencia del servicio de correo electrónico.

Etapa	Descripción
Antes:	• Generar un documento de instalación y configuración del servicio, con todo lo necesario para el funcionamiento de éste. • Monitorear diariamente el funcionamiento y comportamiento del servicio en los dos

	servidores de correo. • Mantener una copia actualizada de los archivos de configuración, así como del *home* y el *var/spool/mail* de todos los usuarios, con sus respectivos archivos de quota. • Mantener una copia de los paquetes y el software relacionados necesarios para instalar el servicio.
Durante:	• En caso de presentarse una situación terminar los procesos y aplicaciones que están funcionando en el servidor. Detener el servicio y guardar la información. • Reiniciar los servicios, si no es necesario el equipo como tal. • Detener las conexiones de red y conexiones activas y reiniciar dichas conexiones. • Iniciar mecanismos para detección y control de accesos no permitidos al equipo. • Restaurar la contraseña de administrador, se deben cambiar si han sido comprometidas. • Instalar un servidor secundario que pueda asumir la responsabilidad del primario, debe ser una réplica capaz de soportar la funcionalidad básica del servicio de correo. • Cuando se debe instalar el sistema operativo se debe instalar la última versión estable, con los respectivos parches de seguridad y actualizaciones pertinentes para esta distribución. • Referirse al documento previamente realizado de instalación y configuración del servicio de correo. • Restaurar información con respecto a usuarios y contraseñas del sistema. • Se deben realizar pruebas del servicio, verificando que los procesos esenciales se encuentran en funcionamiento y consumiendo los recursos necesarios, realizar pruebas para verificar los correos están siendo enviados y recibidos de forma correcta.
Después:	• Restaurar el servidor principal. • Analizar los archivos de logs. • Generar reporte de daños • Reinstalar los servicios si es necesario. • Reinstalar el sistema operativo si es necesario. • Instalar versiones superiores y recientes del software del cual se tiene instalado. • Estudiar la posibilidad de reinstalar nuevo hardware capaz de soportar con mayor eficacia los servicios. • Realizar pruebas para verificar el funcionamiento del correo. • Verificar que los correos están siendo enviados y recibidos de forma correcta. • Verificar el funcionamiento de aplicaciones secundarias como Vsftpd. • Iniciar e instalar el equipo en un lugar seguro, lejos de peligros que lo puedan afectar. • En caso de pérdida total de los archivos, copiar el último backup realizado a los datos de usuarios.

5.3.4 Recuperación del servicio de Proxy-Cache

Tabla 6. 9 Plan de contingencia servicio de Proxy-Cache

Etapa	Descripción
Antes:	• Mantener revisiones semanales de la actualización del software squid. • Se debe realizar revisiones de los recursos, de la utilización del procesador, de memoria, de discos y periféricos de entrada y salida como las tarjetas de red. • Realizar monitoreo diario del servicio, buscando posibles deterioros o sobrecargas del equipo, incluso mal funcionamiento y registrar la información obtenida. • Realizar jornadas de capacitación y difusión de la información y los reportes obtenidos, si en el proceso de análisis se encuentran fallas, estas deben ser comunicadas a los integrantes y administradores, para que se prevean acciones necesarias para estos posibles fallos. • Mantener respaldo de los archivos de configuración del *software* squid.
Durante:	• En caso de falla del servicio en solo uno de los servidores Proxy proceder inmediatamente pasar toda la carga de trafico al que está funcionando. • Si falla el enlace por el que sale un servidor inmediatamente proceder a cambiar sus rutas para que todo su tráfico salga por el otro enlace de red que esté disponible, para esto se encuentran archivos de configuración ejecutables disponibles en cada servidor en /root/bin/routeEmtel y /root/bin/routeETB respectivamente. • Si los servicios fallan por problemas de hardware, se debe contar con equipos que

	permitan funcionar como servidores de respaldo, con la capacidad de soportar la funcionalidad de dicho sistema o servicio. • Si se presenta una situación anormal de falla del servicio, se debe realizar la revisión de los recursos físicos de los cuales hacen uso los servicios, tales como memoria RAM, procesador y espacio en discos. Acudir a la revisión de los logs del sistema para encontrar el origen de la falla. • Si es necesario reiniciar le servicio, • Cuando la falla se presenta por los archivos de configuración, estos deben ser reemplazados por archivos de configuración que se tienen en backup y de los cuales se tiene certeza de su funcionamiento. • Si se encuentran aplicaciones desconocidas o procesos que puedan afectar el desempeño del servicio, dichos procesos deben ser identificados y detenidos manualmente. • Si no es posible restaurar el servicio en el equipo encargado de prestar esta funcionalidad, instalar en un equipo réplica que sea capaz de soportar la funcionalidad básica.
Después:	• Evaluar las pérdidas que se presenta en cuanto a procesador, memoria, discos duros, tarjetas de red y el funcionamiento y desempeño de los recursos debido a problemas con los servicios o aplicaciones desconocidas. • Reemplazar en el menor tiempo posible el software y los elementos que se encuentran fallando, para este caso verificar si el software tiene soporte, si lo tiene contactar al soporte para de esta manera obtener una versión de software estable. Si es necesario instalar software con las actualizaciones o versiones actuales. • Realizar actividades para reinstalación en primer estancia de los servicios, si este procedimiento no se puede llevar a cabo debido a problemas del sistema operativo realizar la reinstalación del mismo, para esto tener en cuenta instalar las versiones y el software adecuado y requerido. • Iniciar los servicios y restaurar los datos que involucran usuarios externos y elementos importantes del sistema. • Verificar que los servicios están en correcto funcionamiento. • Verificar la posibilidad de instalar nuevas versiones o actualizaciones de seguridad. • Generar un documento en el cual se consigne la información referente a las fallas que se han presentado y la solución que se le ha dado, asimismo enmarcar la efectividad de los procesos utilizados.

6 Plan de pruebas

6.1 Introducción

El plan de pruebas se realiza para poder confrontar los resultados obtenidos en el proceso de diseño de las políticas de seguridad y el plan de contingencia para el Centro de Datos de la Universidad del Cauca, se trata de constatar cómo pueden ser aplicados los controles, verificar su resultado y eficacia, para de esa manera generar las recomendaciones que mejoren la gestión de la seguridad de la información. La realización de este plan de pruebas emplea algunos de los elementos que se pueden encontrar en un denominado *test* de intrusión, ya que al igual que este la idea y finalidad es evaluar el estado de los sistemas, equipos y el personal frente a situaciones anormales. Una de los mejores maneras de probar la fortaleza y las debilidades de un sistema, es tratando de llevar a cabo situaciones que debiliten o entorpezcan su funcionamiento, en cierta medida esto puede denominarse como un *hacking ético*, en el cual se pretende realizar ataques para detectar posibles focos de inseguridad. [58]

El plan de pruebas propuesto con el fin de verificar las políticas y el plan de contingencia, será aprobado y estará enmarcado dentro de los límites que el administrador del Centro de Datos considere necesarios, importantes y que por sus características económicas y de disponibilidad de recursos y de personal puedan ser implementados de una manera inmediata.

6.2 Pruebas de intrusión

Cuando se realizan pruebas de intrusión, es conveniente tener una base, para esto se han desarrollados metodologías que ayudan en este proceso, una muy importante y difundida para estos procesos y que es ampliamente utilizada es OSSTMM[21] [59], la cual provee los pasos necesarios para poder realizar pruebas y ataques de seguridad a la información con miras a obtener resultados que permitan mejorar los niveles de seguridad.

[21] OSSTMM: open source testing methodology Manual [2].

Para la realización de pruebas, captura de información e incluso ataques a los elementos de estudio, se han definido actualmente algunos métodos y caminos que por sus características dan enfoques diferentes de la manera como se realizarán las pruebas de intrusión figura 5.1, por una lado se tiene el método *Black box*[22], en el cual se parte del hecho que no se conoce información alguna sobre el sistema al cual se le realizarán las pruebas, se tienen también el método W*hite box*[23], en el cual se tiene información relevante del elemento a ser estudiado, se conoce la infraestructura, los modos de operación y de funcionamiento, incluso información sensible referente al personal, igualmente se tienen algunas variables como por ejemplo G*ray box*[24] del cual se conoce información parcial. Es importante mencionar que las pruebas de intrusión pueden realizarse de manera completa o manera parcial según se defina, para este caso los resultados están enmarcados por la información entregada por el administrador del Centro de Datos. Para el análisis se empleará el método *white box* ya que las personas que lo van a realizar tienen conocimiento pleno de la infraestructura y la información que se maneja actualmente.

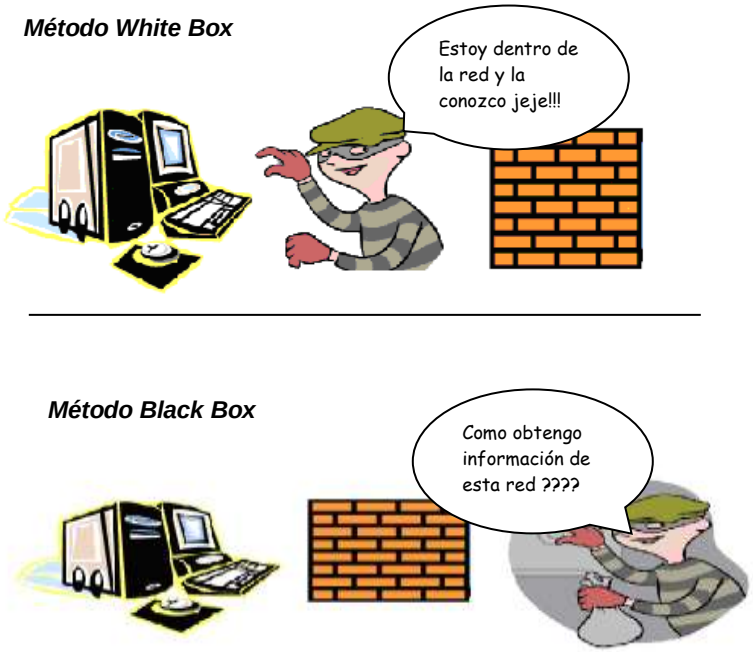


Figura 5. 1 Pruebas de intrusión

[22] Black box: Caja negra. Método para realizar pruebas a los sistemas de seguridad cuando no se conoce información de la entidad objeto de estudio.
[23] White box: Caja blanca. Método para realizar pruebas a los sistemas de seguridad cuando se conoce la suficiente información de la entidad objeto de estudio.
[24] Gray Box: Caja gris. Combinación entre la técnica white box y black box.

OSSTMM: está metodología requiere y propone algunos elementos y pautas para recolección de información, que al tenerla en cuenta permiten obtener mejores resultados de los elementos y pruebas realizadas, algunos de estos a tener en cuenta son:

- Fecha y hora de las pruebas.
- Duración de las pruebas.
- Auditores y analistas que intervienen en las pruebas.
- Tipos de pruebas.
- El alcance.
- Método para clasificar y enumerar las pruebas.
- Verificación de las pruebas y las métricas para calcular los niveles de protección, las pérdidas de controles y las limitaciones de seguridad.
- Todas las pruebas realizadas, las no realizadas y las que parcialmente se han realizado.
- Márgenes de pruebas y errores.
- Los procesos que influencian los límites de seguridad que se manejan.
- Cualquier edición con respecto a las pruebas y la validación de resultados.
- Conocimiento de posibles anomalías.

OSSTMM proporciona las siguientes recomendaciones a tener en cuenta para realizar pruebas de seguridad a sistemas informáticos, de manera global en la figura 5.2 se pueden observar los criterios recomendados:

- Las pruebas deben realizarse lo más completas posibles.
- Las pruebas deben incluir a todos los grupos interesados y el personal necesario.
- Las pruebas realizadas deben estar conforme a la normatividad y legislación del país o el ente educativo.
- Los resultados deben ser cuantificables y medibles.
- Los resultados deben ser constantes y se deben poder replicar en otro ambiente.
- Los resultados deben tener información únicamente de las pruebas realizadas.

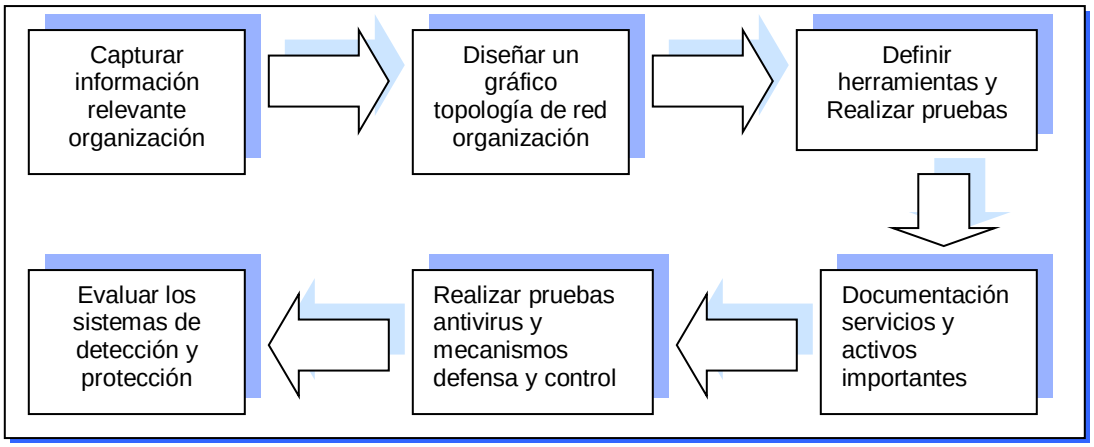


Figura 5. 2 Criterios recomendados para un plan de pruebas

Por otro lado al realizar pruebas de intrusión o pruebas de seguridad, es conveniente tener en cuenta criterios adicionales como: [60]

Tabla 5. 1 Criterios plan de contingencia

No	Criterios recomendados
1	Realizar un sondeo de la red, con el fin de obtener una topología y mapa aproximado de la infraestructura que será objeto de estudio. Se puede realizar un escaneo de puertos de identificación de servicios y sistemas operativos que se tienen en la red.
2	Realizar pruebas para detectar posibles vulnerabilidades, esto con la ayuda de herramientas destinadas a esta función.
3	Realizar pruebas para descifrar contraseñas, asimismo se pueden emplear elementos para probar contraseñas con usuarios por defecto del sistema y se pueden emplear ataques de fuerza bruta para descifrar esta información.
4	Realizar una documentación muy completa con información relevante de los servicios, servidores y el personal de tal manera que se pueden emplear mecanismos para descifrar esta información.
5	Mantener y realizar pruebas de antivirus para determinar la eficacia y el nivel de defensa que ofrecen a los equipos que ellos protegen.
6	Categorizar y describir las vulnerabilidades de los sistemas y servidores, asimismo determinar las relaciones o elementos de confianza, tales como llaves compartidas que permiten acceso de un equipo o de un sistema sin requerir confirmación.
7	Probar los planes de contingencia o medidas de contención que permiten actuar frente a situaciones anormales.
8	Verificar las políticas de seguridad de la información existentes, para determinar si cumplen con los elementos necesarios para garantizar la privacidad de la información.
9	Realizar pruebas de forma manual de las posibles vulnerabilidades que afectan los sistemas y las cuales no pueden ser detectadas por los sistemas o herramientas empleadas para este fin.
10	Verificar el sistema de detección de intrusos, a fin de estudiar su funcionamiento y el nivel y la eficacia de las respuestas.
11	Definir problemas que se puedan presentar por aplicaciones, por ejemplo aplicaciones Web para gestión de contenido.

6.3 Importancia de establecer un plan de pruebas

Un plan de pruebas permite verificar de una manera más concreta los resultados obtenidos de un proceso de análisis y diseño de mecanismos de seguridad, para este caso concreto

permite verificar el análisis y diseño de las políticas de seguridad, y el plan de contingencia propuesto a lo largo del proyecto. Permite adicionalmente determinar la eficacia de los mecanismos, la facilidad de la implementación de los mismos y la relación costo beneficio que implica la implementación o no de los mismos con respecto a los servicios, servidores y el personal, por otro lado poder realizar una implementación y prueba de la misma, permite obtener resultados, que con el respectivo análisis permitirá introducir mejoras que ayudarán a incrementar el nivel de la seguridad que se maneja en los sistemas de información.

6.4 Criterios establecidos para el plan de pruebas

En esta parte se establecerán los criterios mínimos sugeridos para la realización de un plan de pruebas que se pueda aplicar a un centro de datos, cabe destacar que queda a disposición de los desarrolladores el uso de los criterios que más se acoplen a su proyecto. En la figura 5.3 se pueden observar las diferentes etapas que se pueden cumplir.

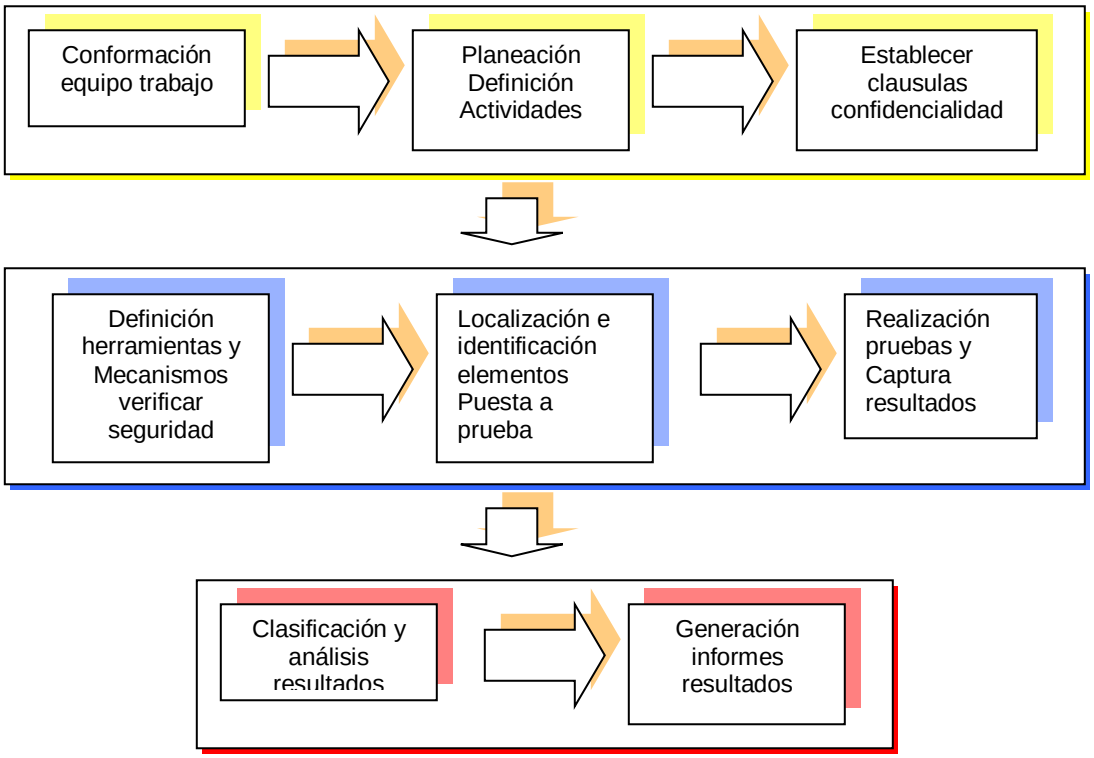


Figura 5. 3 Criterios recomendados para el Centro de Datos

Tabla 5. 2 Criterios para el plan de pruebas aplicados al Centro de Datos

Nº	Criterios para realizar pruebas de seguridad
1	Conformación de un grupo de trabajo, encargado de realizar las pruebas, estudiar los resultados obtenidos y generar una aprobación o no del procedimiento realizado.
2	Definir el límite y alcance de las pruebas, delimitando claramente los objetivos propuestos y los

	resultados obtenidos como por ejemplo: delimitar qué tipo de políticas o estrategias de plan de contingencia serán tenidas en cuenta para ser aplicadas, asimismo definir que se quiere obtener al realizar dichas pruebas, sin olvidar de enmarcar el alcance y los elementos que serán comprometidos en dicho proceso.
3	Establecimiento de un cronograma, definiendo claramente aspectos como: el tiempo de inicio, el tiempo requerido para realizar las pruebas y el tiempo propuesto para la finalización de las actividades propuestas.
4	Definición clara de los criterios de valoración o indicadores que permitirán medir los resultados obtenidos para cada etapa del proyecto.
5	Definir de manera clara la forma y entrega de resultados, así como la manera de la presentación y almacenamiento de los mismos.
6	Un factor importante a tener en cuenta es el grado y las cláusulas de confidencialidad que se le deben dar a la información obtenida.
7	Identificar los equipos y elementos a los cuales se realizarán las pruebas.
8	Definir las herramientas y elementos necesarios para llevar a cabo las pruebas, se pueden emplear herramientas para análisis y ejecución de vulnerabilidades, para con esto definir y obtener los resultados necesarios.
9	Identificación de las políticas de seguridad y el plan de contingencia que se emplearán como objeto de estudio para validar la eficacia y la necesidad o no de la implementación de las mismas de manera permanente. Las pruebas definidas para poder validar este proceso deben ser avaladas y aprobadas por el administrador de los servicios.
10	Definir las pruebas que se realizarán, se debe consignar de forma clara y expresa la manera como se espera obtener resultados, así mismo como se espera que se reaccione ante las situaciones provocadas por estos elementos.
11	Las pruebas que se realizarán sobre los servidores, equipos e instalaciones físicas, deben ser realizadas en horarios en los cuales el impacto que puede causar su implementación sea bajo, para esto se deben elegir horarios no laborales o de poca afluencia en el uso de los recursos.
12	Antes de realizar las pruebas, es conveniente tener y garantizar una copia de los archivos de configuración y de los datos contenidos e involucrados con los servidores de prueba.
13	Las pruebas deben garantizar que no ocasionarán daños físicos o irreversibles sobre los equipos que se han dispuesto para este fin.
14	Las pruebas deben contar y determinar un intervalo de tiempo prudente en el cual se sacarán de funcionamiento los servicios, el intervalo de tiempo y frecuencia empleado para realizar las pruebas debe estar acorde al cronograma y al umbral permitido y aprobado previamente.
15	Cuando se realizan pruebas se debe contar con el personal adecuado, capaz de restaurar los servicios y los equipos en el menor tiempo posible.
16	La realización de los pruebas implica interrupción de los servicios en algunos casos, por lo tanto se debe emplear un medio de comunicación eficaz para informar a los usuarios que se llevará a cabo este proceso de tal manera que ellos no se vean afectados por estas pruebas.
17	Las pruebas que se realizan en lo posible deben tener en cuenta los diferentes perfiles de usuarios, es decir: usuarios externos, usuarios internos de la organización e incluso como si fuera el propio administrador de los sistemas.
18	Si se emplean herramientas o mecanismos para realizar pruebas de servicios o equipos, se debe realizar un proceso de revisión y adecuación de tal manera que se puedan dejar los servicios con la debida protección y con los debidos elementos de seguridad que mitiguen posibles daños generados.
19	Emplear herramientas para análisis de vulnerabilidades, que permitan obtener información del funcionamiento y las características de seguridad actual de los servidores y servicios a tener en cuenta, para esto se pueden emplear herramientas como Nessus, Nmap, el empleo de dichas herramientas de ser avalado y permitido por administrador de los servicios, ya que el uso de las mismas implica un ataque de seguridad.
20	El uso de herramientas para explotar las vulnerabilidades encontradas, debe ser debidamente documentado, definiendo el uso y alcance de los mismos.
21	A los equipos y servicios involucrados en las pruebas, se les debe realizar un análisis de recursos físicos y lógicos, discriminando claramente cómo se ven afectados en su desempeño y funcionamiento, a fin de determinar su capacidad de respuesta ante posibles inconvenientes.
22	Los resultados deben ser claramente identificados y propuestos de tal manera que se pueda llevar a cabo un proceso de confrontación, para mejorar o realizar una reestructuración de los elementos puestos a pruebas, para este caso las políticas y el plan de contingencia.
23	Presentar conclusiones y recomendaciones de acuerdo a los planes y resultados obtenidos.
24	Las herramientas o elementos que puedan poner al descubierto información sensible tal como

	información personal deben tratarse con cuidado, ya que es información clasificada y por tal razón no debe ser manipulada ni expuesta a ser accedido por entes externos.
25	Las pruebas se deben realizar sobre un ambiente controlado, si el impacto de estas pruebas es muy alto, dichas situaciones se deben simular en la medida de las posibilidades teniendo en cuenta los datos reales.
25	El plan de pruebas se debe acoplar a las características de la institución y a las políticas y plan de contingencia previamente definido, para esta manera poder confrontar la eficacia de estos.
26	Las aplicaciones de servicios que son esenciales y que no pueden ser detenidos o interrumpidos deben ser sometidos a pruebas asumiendo situaciones probables y de acuerdo a esto valorar los posible resultados.
27	Establecer las condiciones de funcionamiento de los dispositivos, para de esta manera simular que los elementos están funcionando al máximo de su capacidad.
28	Definir y documentar claramente el funcionamiento de los sistemas frente situaciones adversas, de igual manera definir el funcionamiento de los sistemas en cuanto a cómo responden frente a determinadas situaciones.
29	Establecer cómo reacciona el sistema ante una falla, para establecer y elegir claramente cómo puede corregirse o tratarse dicha situación.
30	Establecer claramente las causas y efectos de las pruebas realizadas sobre los servidores y servicios.
31	Determinar cómo reacciona el personal y determinar si están preparados para afrontar situaciones anormales.

7 Anexo plan de pruebas

7.1 Desarrollo plan de pruebas

7.1.1 Conformación del equipo de trabajo

El equipo de trabajo conformado para revisar las pruebas, se definió similar al equipo conformado para revisar las políticas y plan de contingencia de esta manera se define lo siguiente:

Coordinador: Administrador servicios y servidores de Internet Universidad del Cauca.
Diseñador 1: Estudiante de proyecto de grado.
Diseñador 2: Estudiante de proyecto de grado.
Evaluador 1: Administrador servicios y servidores de Internet Universidad del Cauca.
Asesor: Docente departamento de sistemas Universidad del Cauca, especialista en seguridad informática.

7.1.2 Límites y objetivos

Las pruebas que se realizarán al Centro de Datos, están definidas exclusivamente para comprobar la implementación de algunas políticas y algunos criterios establecidos en el plan de contingencia, estas políticas y criterios serán definidos previamente por el administrador de los servicios, quien hará recomendaciones pertinentes según las cuales se deben o no implementar.

Las pruebas no generaran daños sobre los sistemas ni sobre el hardware ni el software, tampoco afectarán la continuidad en la prestación de los servicios, por tal motivo estas pruebas se realizarán únicamente a los servidores y equipos en los cuales se puedan simular situaciones anormales.

7.1.3 Indicadores de operación

Están definidos por los resultados obtenidos a lo largo el proyecto, es decir se medirán las herramientas en cuanto a la información obtenida con estas. El análisis de esta información

permitirá encontrar posibles mejoras al plan de contingencia propuesto y a las políticas diseñadas. Se espera con estas pruebas obtener un documento en el cual se consignen los resultados obtenidos y se confronten con respecto a las políticas y el plan de contingencia que se tiene actualmente planteado.

7.1.4 Cláusulas de confidencialidad

La información obtenida en el desarrollo de las pruebas debe tratarse como información confidencial, por lo tanto esta información es importante únicamente para los administradores del Centro de Datos, por tal razón los resultados expuestos y presentados en el documento son análisis estadísticos donde se muestra los posibles resultados de la implementación de controles y políticas establecidas para la seguridad de la información.

7.1.5 Actividades a realizar

Las pruebas se realizarán aplicando las respectivas herramientas para obtener la información, se definieron los siguientes puntos para su realización:

1. Las herramientas empleadas serán aplicadas a servidores tales como el servidor WEB, servidores Proxy, DNS y servidores de correo electrónico.
2. Se realizarán pruebas para descifrar contraseñas tanto de estaciones de trabajo como servidores y equipos de red. Para esto se emplearan herramientas como Jhon the Ripper, con el fin de determinar la facilidad y complejidad de los mecanismos empleados para la creación de contraseñas. Para éstos se emplearan los archivos *Passwd* y *Shadow* previamente cedidos por el administrador del sistema, está pruebas se realizarán para una estación de trabajo y un servidor principal, para este caso será el servidor Web. Se espera poder confrontar las políticas de seguridad referentes a la creación de contraseñas y los cuidados mínimos que se tiene.
3. Se realizará una verificación de la documentación, de tal manera que se pueda verificar si se encuentra actualizada la información referente a los servidores estudiados tales como el servidor Web, Proxy, DNS y el servidor de correo, para ésta manera confrontar la política de seguridad la cual implica una actualización permanente de la documentación que se cuenta para los servicios y servidores.

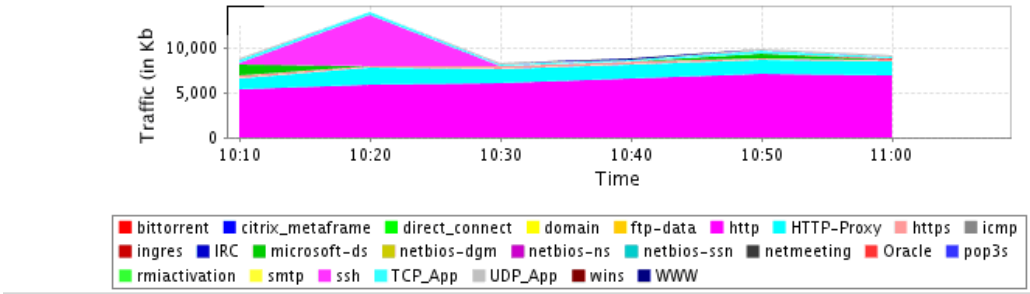
4. Se verificará los medios de protección con los cuales cuentan los servidores y estación de trabajo tales como antivirus o elementos como firewalls. Con el fin de confrontar la seguridad en lo referente a mecanismos de protección, puertos y servicios que se tienen bloqueados o autorizados. Para ésta manera confrontar si con la realización del análisis de riesgos estos inconvenientes fueron tenidos en cuenta.
5. Se verificará las políticas creadas en lo referente a la información personal de cada usuario de tal manera que se puede confrontar las políticas que garantizan la confidencialidad, la integridad y la disponibilidad de la información.
6. Se verificará el funcionamiento del sistema detector de intrusos instalado como política de seguridad para determinar qué tan expuestos se encuentran los servicios y servidores a una posible situación de riesgo.
7. Se realizarán pruebas con respecto a posibles errores humanos que pueden introducir fallas en los servicios y servidores tales como borrado de archivos, daño de software. Se espera esta manera poder verificar el plan de contingencia diseñado para permitir retornar a normal funcionamiento los servicios y servidores en el menor tiempo posible.
8. Si se encuentra alguna vulnerabilidad conocida se tratará de realizar un acceso no permitido a través de herramientas creadas para realizar ataques de acceso a los equipos con el fin de generar posibles soluciones.

7.1.6 Resultados de las pruebas aplicadas al Centro de Datos

Primero: Verificar el uso de aplicaciones P2P en horarios laborales y horarios no laborales, para esto se empleo la información entregada por herramientas como: el Netexplorer, Netflow y Mrtg, información que se puede visualizar de manera gráfica y permite obtener un consolidado de la cantidad y el tipo de tráfico que está circulando tanto en la red interna como en la red externa, la cual permite el acceso a Internet. Estas pruebas se realizaron dentro de los horarios establecidos en horas pico para determinar que realmente las restricciones y los horarios funcionan de acuerdo a las aplicaciones que están permitidas en esa brecha de tiempo.

Del análisis en horas pico y en horas no laborales se obtuvo como resultado satisfactorio que los controles establecidos permiten cumplir esta política, esto se verificó con la información entregada por las herramientas de gestión en los horarios laborales, en estos horarios el

tráfico IP que predomina es el correspondiente a la navegación por vía Proxy. Asimismo en horarios no laborales comprendidos entre las siete de la noche y las seis de la mañana se puede observar que incrementan en cierto porcentaje los aplicaciones para descarga de información, igual sucede los fines de semana. Políticas aplicadas: administradores 1, 44, 45, 46 y 47; usuarios 40, 42 y 43. En la figura 7.1 se observa el tráfico de la red interna, suministrado por la herramienta Netflow Analyzer, se comprueba que el protocolo de mayor uso es el http y http-proxy.



Showing 1 to 50 View per page 50

Application	Traffic(Total: 4387.35 MB)	Percentage of total traffic
http	2822.87 MB	64%
HTTP-Proxy	689.93 MB	16%
ssh	437.63 MB	10%
microsoft-ds	125.54 MB	3%
TCP_App	122.04 MB	3%
https	107.01 MB	2%
UDP_App	44.71 MB	1%
WWW	7.29 MB	<1%
domain	6.48 MB	<1%

Figura 7. 1 Tráfico red Interna

Las figuras 7.2 y 7.3 muestran el consumo sobre el ancho de banda realizado por los servidores, suministrada por la herramienta de gestión Netexplorer, se comprueba que el mayor tráfico es el del equipo Proxy para acceso a Internet.

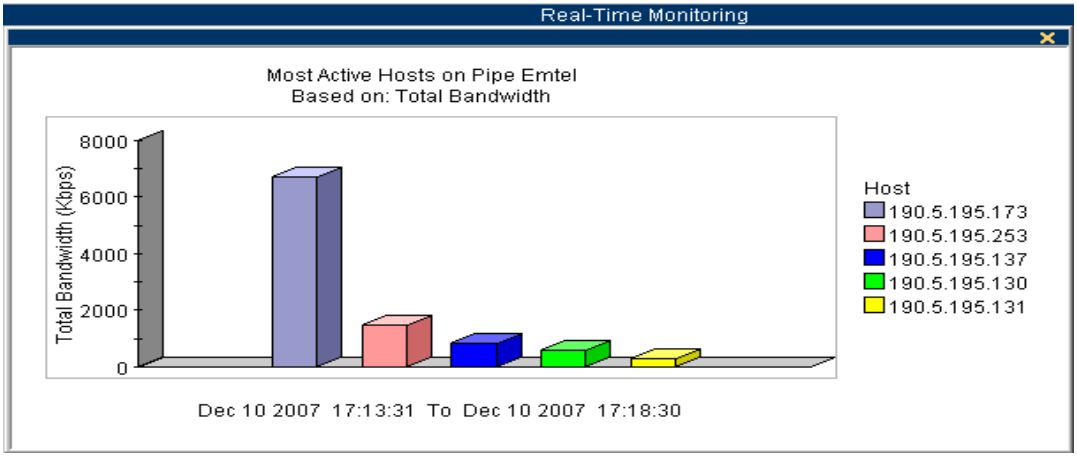


Figura 7. 2 Consumo ancho de banda

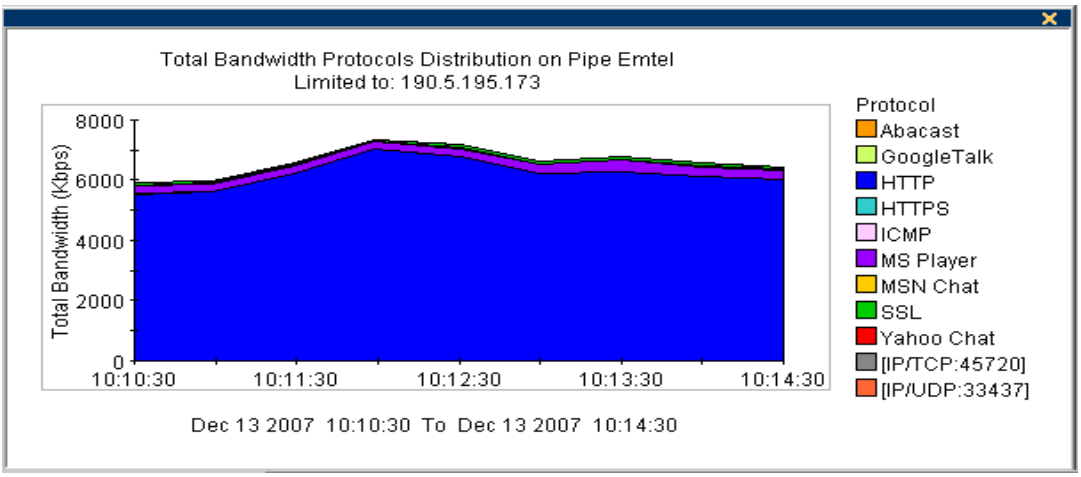


Figura 7. 3 Tráfico servidor Proxy

En las figuras 7.4 y 7.5 se observa el tráfico de los enlaces hacia Internet con los que cuenta la Universidad, el tráfico entrante y el saliente.

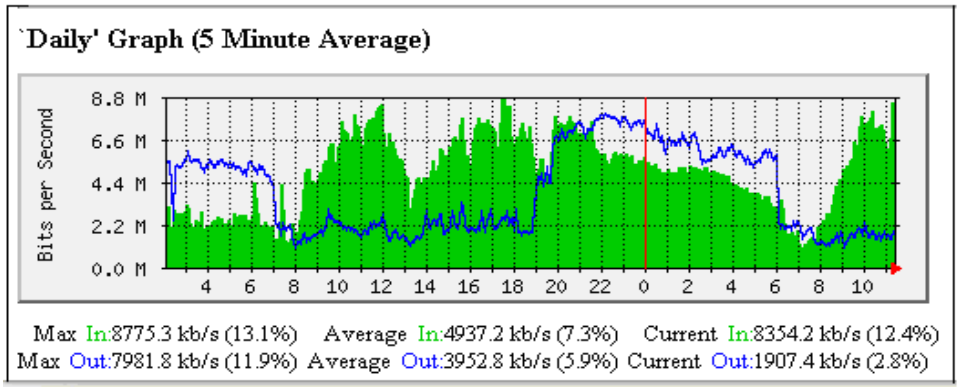


Figura 7. 4 Tráfico enlace principal con Emtel

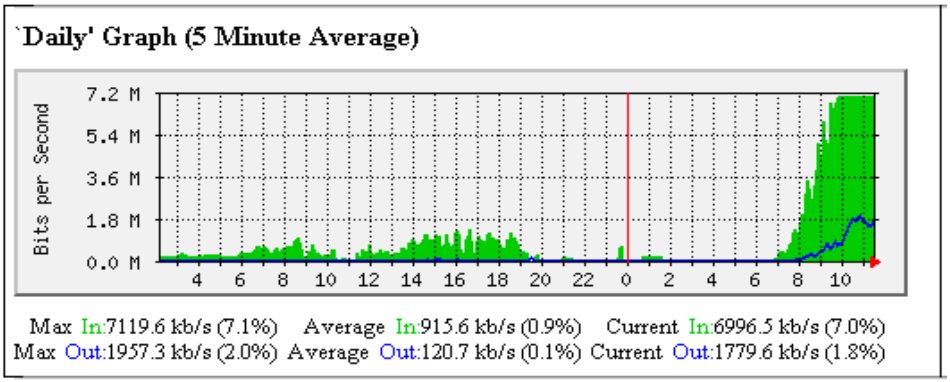


Figura 7. 5 Tráfico enlace secundario con ETB

Segundo: Es importante mantener una monitorización diaria del funcionamiento de los servicios, para con esto constatar que los servicios son analizados y estudiados de manera constante, este proceso actualmente se realiza con herramientas como Nagios, Netflow, MRTG que están entregando reportes y gráficas del funcionamiento de los recursos y elementos con los que cuenta el Centro de Datos. Se comprobó que mantener estas herramientas garantiza que los servicios están en óptimas condiciones, cuando ocurre un inconveniente el tiempo empleado en detectar y dar una respuesta es muy corto. Política aplicada 4. Las figuras 7.6 y 7.7 muestran las estadísticas de utilización del servicio de correo electrónico. La figura 7.8 muestra el monitoreo que se le realiza a los servidores con la herramienta Nagios

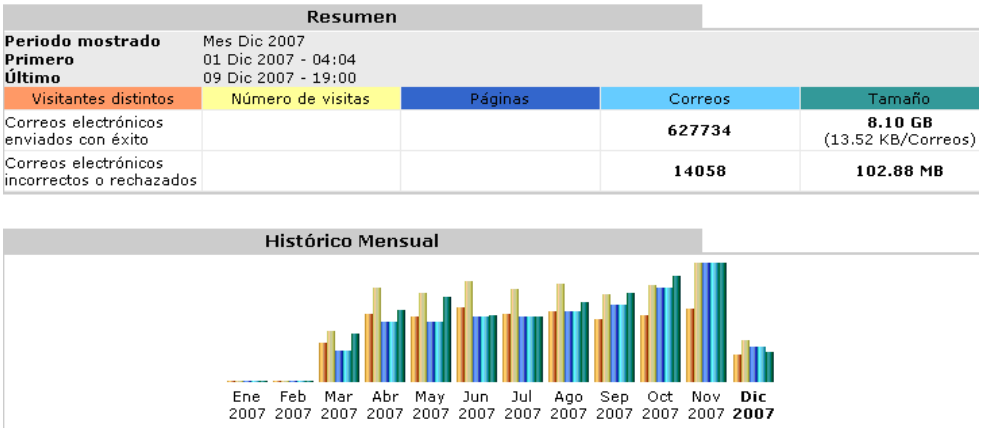
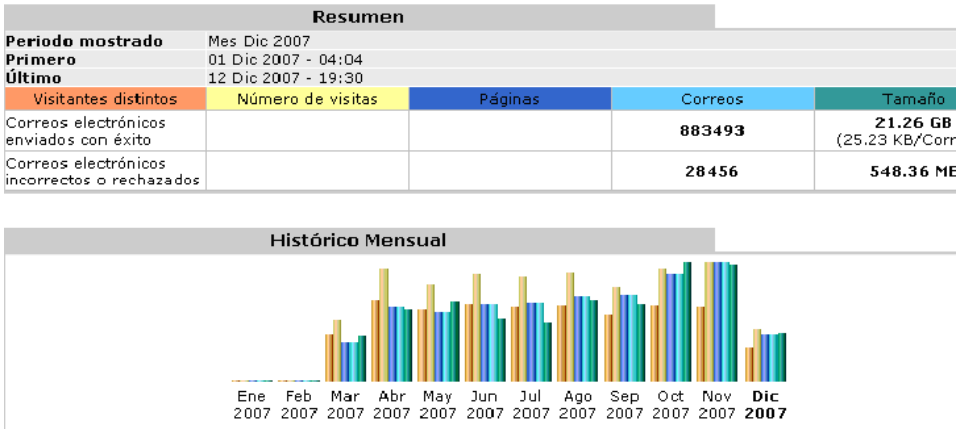


Figura 7. 6 Servicio de correo electrónico



Resumen

Periodo mostrado	Mes Dic 2007			
Primero	01 Dic 2007 - 04:04			
Último	12 Dic 2007 - 19:30			
Visitantes distintos	Número de visitas	Páginas	Correos	Tamaño
Correos electrónicos enviados con éxito			**883493**	**21.26 GB** (25.23 KB/Corr
Correos electrónicos incorrectos o rechazados			**28456**	**548.36 MB**

Histórico Mensual

Figura 7. 7 Servicio de correo electrónico

.

Figura 7. 8 Monitoreo servidores

Tercero: Los archivos de sucesos o archivos del sistema permiten verificar las acciones que han ocurrido en el sistema y a los servicios es por esto tan importante que se estén generando y que estén disponibles para los administradores cuando lo requieren. Por esto por medio de estos se pretende verificar que realmente sobre los servidores y servicios se está llevando un control adecuado en factores como apagado de los equipos, reiniciado del sistema, de los servicios. Este proceso actualmente es algo difícil de realizar ya que se tiene que analizar de forma manual los archivos. Se constato que los archivos se están generando tanto para el sistema como para las aplicaciones y estos archivos cuentan con los permisos necesarios para que los administradores los puedan acceder.

Asimismo se verificó que los usuarios y los destinos de las conexiones esto se puede constatar al mirar el número de los puertos y ser analizados los destinos donde se corroboró que están conectadas usuarios válidos y destinos conocidos, se encontró esporádicamente usuarios conectados demasiados tiempo. Políticas aplicadas: administradores 10 y 11; usuarios 47.

Cuarto: El restablecimiento de copias de seguridad que actualmente se está realizando, es máximo de una semana, es decir, el usuario que solicita el restablecimiento de la información de su correo sólo lo puede obtener hasta de ocho días antes. Para esta prueba se tomó un usuario y se restablecieron las copias de seguridad tanto para su correo como para su sistema de archivos, lo cual verificó que estas copias eran de la semana pasada. En esa parte se tiene un inconveniente y está relacionado con el tiempo máximo que se puede guardar una copia de seguridad, lo ideal es que el tiempo de almacenamiento sea un poco más amplio, este proceso se está realizando con copias en el servidor Ftp y en el Intercambiador de cintas. Políticas aplicadas: administradores 18, 89.

Quinto: Dentro de los parámetros que se tienen para los usuarios que hacen uso del servicio de correo electrónico, se mantienen unos que definen la capacidad de almacenamiento máximo, para esto se tomaron los usuarios del servidor de estudiantes y del de docentes para verificar el espacio asignado y el sistema de aviso para indicar que están sobrepasando el límite establecido, de esto se obtuvo que el sistema de quotas para los usuarios está funcionando. Políticas aplicadas: administradores 17, 31, 86, 87; usuarios 4.

Sexto: Verificación del funcionamiento de los equipos empleados como Proxys, los cuales son fundamentales para la navegación a Internet de casi la totalidad de usuarios. Se verificó que efectivamente se bloquean las aplicaciones no permitidas que son empleadas para descarga de información, también se realizó un estudio del estado de los equipos que soportan el servicio Proxy constatando que están en condiciones de soportar la capacidad y rendimiento al número de peticiones que está recibiendo actualmente figura 7.9 y 7.10, donde se aprecia que se maneja un promedio de 2 Megas. Políticas aplicadas 21, 22.

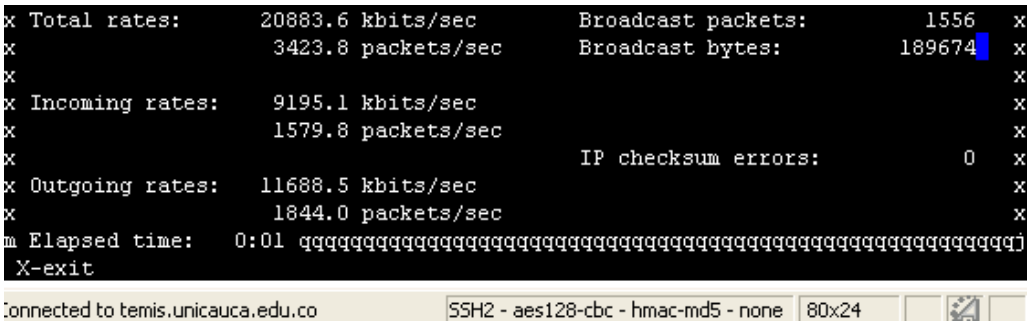


Figura 7. 9 Tráfico interfaz Proxy Temis

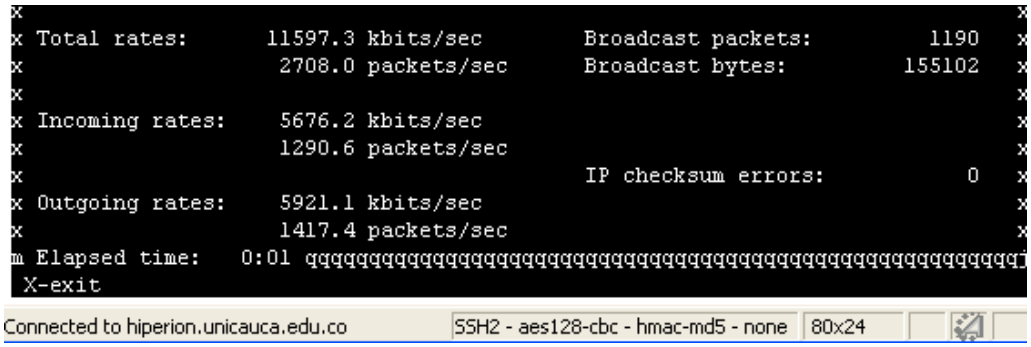


Figura 7. 10 Tráfico interfaz Proxy Hiperion

Séptimo: Verificación de la información mantenida en el Ftp, este servicio por ser de carácter institucional y estar disponible para Internet, la información mantenida solo puede ser de contenido educativo. De esto se obtuvo que se tiene software no permitido, específicamente con herramientas como antivirus y software de desarrollo. Políticas aplicadas: administradores 29 y 30; usuarios 16 y 17.

Octavo: Cuando sale de funcionamiento el portal institucional es importante mantener una página de pruebas que permita visualizar un mensaje correspondiente a que esta fuera de servicio y que se está trabajando para resolver el inconveniente, esto se realizó montando sobre una estación de trabajo una página de prueba y redireccionando sobre esta página cuando se presenta la falla. Política aplicada 37.

Noveno: En cuanto a los usuarios que hacen uso de los servicios y servidores que ofrece el Centro de Datos es necesario verificar que cuentan con la posibilidad de realizar las acciones necesarias para poder realizar sus funciones básicas, asimismo se verifico que ellos cuentan con los permisos necesarios de tal manera que no tengan privilegios adicionales con los cuales puedan ocasionar fallos o errores de formación de los usuarios o incluso el sistema.

Como resultado de este análisis se obtuvo que con los permisos de los archivos solo los propietarios de la información la puedan modificar. Un inconveniente que se presenta es por los usuarios que acceden a los servicios y servidores ya que de esta manera se incrementa los posibles fallos de seguridad. Política aplicada 198.

Decimo: Actualmente se presta el servicio de hosting y alojamiento en bases de datos, por seguridad se deben realizar permanentes monitoreos a estos sitios para evitar posibles inconvenientes que puedan generar fallos en las aplicaciones, es por esto que se tomó algunos sitios de referencia y se revisaron los permisos que cuentan de tal manera que se encontraron algunos sitios de usuarios con los permisos tanto de lectura como de escritura abiertos, es decir cuentan con la posibilidad de ser modificado por cualquier usuario. Asimismo se realizó verificación del contenido que es mantenido en estos sitios de tal manera que esta información se confronto y se obtuvo que de la totalidad de los sitios de la Universidad alojados en el servidor institucional, se tiene un conocimiento de un 92.75 % sobre los administradores responsables de ellos (262, 19) y un 16% han sido asignados pero no utilizados (262, 42). Respecto al contenido de los sitios se encontró que un 1,9% tienen información no permitida (música) Política aplicada usuarios 57.

Once: Uno de los factores importantes para garantizar la seguridad de la información es la creación de contraseñas robustas, para verificar esto se tomaron los archivos de *Password y Shadow* de uno de los servidores principales y se empleo el programa Jon The Ripper para de esta manera tratar de descifrar las contraseñas. Al respecto se encontraron contraseñas de fácil desciframiento las cuales se recomendó cambiar inmediatamente. De las estaciones de trabajo y de los servidores principales se encontró que las contraseñas de root cuentan con un mecanismo de elaboración que las hacen mucho más difícil de descifrar. Los resultados del procedimiento realizado al servidor Web se muestran en la tabla 7.1. Políticas aplicadas: administradores 201, 203, usuarios 66.

Tabla 7. 1 Verificación de contraseñas

Usuarios con contraseña comprometida	Acciones	Resultado
8	Eliminados.	Eliminados.
4	Envío correo; Cambio de contraseña.	Confirmación responsable, envío de la nueva contraseña.
6	Envío correo; Cambio de contraseña.	A la espera de la respuesta.

Doce: Un factor importante dentro de este proceso es la documentación que se está realizando sobre la configuración e implementación de servicios, es importante garantizar para los encargados de gestionar el sistema, acceder a la documentación, que este actualizada y que el acceso sea de una manera rápida y segura, en el caso de presentarse alguna falla y se requiera restablecer un servicio. Se encontró que la documentación está parcialmente actualizada y alguna aún no existe. Políticas aplicadas administradores 78-85, 234.

Trece: Es importante mantener un cronograma de trabajo durante todo el año en el cual se cubran aspectos importantes de los diferentes procesos que se estén realizando en la Universidad y los cuales hacen uso de los servicios y servidores. El cronograma permite planificar y estructurar los posibles periodos en los cuales se realizará mantenimiento preventivo, correctivo, cambios en los equipos, para de esta manera garantizar un óptimo funcionamiento y que no se entorpezcan actividades. Políticas aplicadas administradores 106, 113, 130.

Catorce: Analizar los intentos de intrusión junto con la detección de virus permite una mejor visión sobre la importancia de la seguridad en las redes de comunicaciones, ya que de no contarse con los elementos como firewalls y antivirus que protegen de estos ataques se sufrirían varios daños que pueden perjudicar en gran medida la prestación de los servicios. Las tablas 7.2, 7.3 y 7.4 muestran la cantidad de virus detenido hacia los servidores, el tipo de virus, la fuente de origen y el destino, se observa que los servidores de correo son los más atacados por este tipo de elementos.

Tabla 7. 2 Detección de virus

Dirección del ataque	Nombre del virus	Número de eventos
Entrada	W32/Small.C5C5@mm	1958
	HTML/BankFraud.OD!phish	1514
	W32/Agent.NAF!tr	1494
	Other(21)	1321
Total		**6287**

Tabla 7. 3 Origen de virus

Dirección del ataque	Fuente	Número de eventos
Entrada	200.118.166.195	54
	bay0-omc1-s13.bay0.hotmail.com	17
	c416-19.Impsat.com.co	15
	Other(5241)	6256
Total		**6342**

Tabla 7. 4 Destino de virus

Destino	Número de eventos por día
Atenea	2802
Afrodita	2089
Acuario	25

En las figuras7.11, 7.12 y en la tabla 7.5, se puede observar el tipo de ataques realizados y el destino de estos, El mayor tipo de ataque es debido la base de datos MSSQL, que en ocasiones ya se ha tenido la oportunidad de constatar cómo este tipo de fallos sin contar con la debida protección han causado el entorpecimiento de la red interna, afectando por tanto la prestación de todos los servicios.

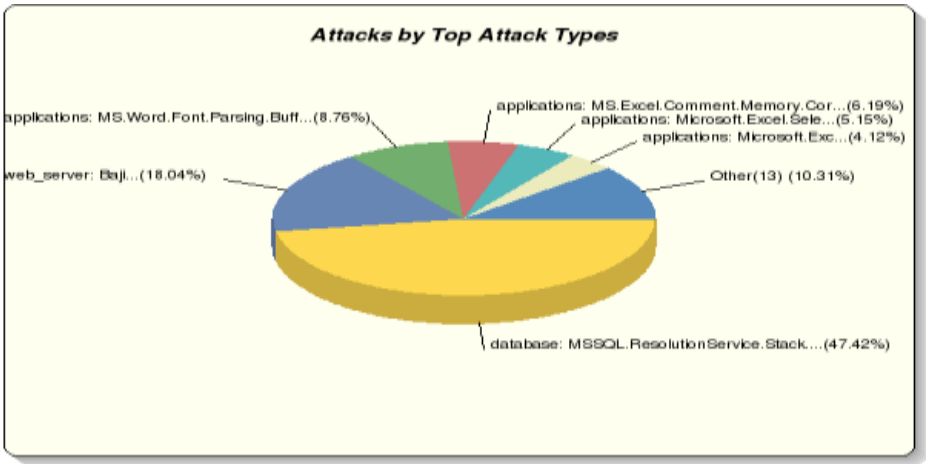


Figura 7. 11 Tipo de ataques

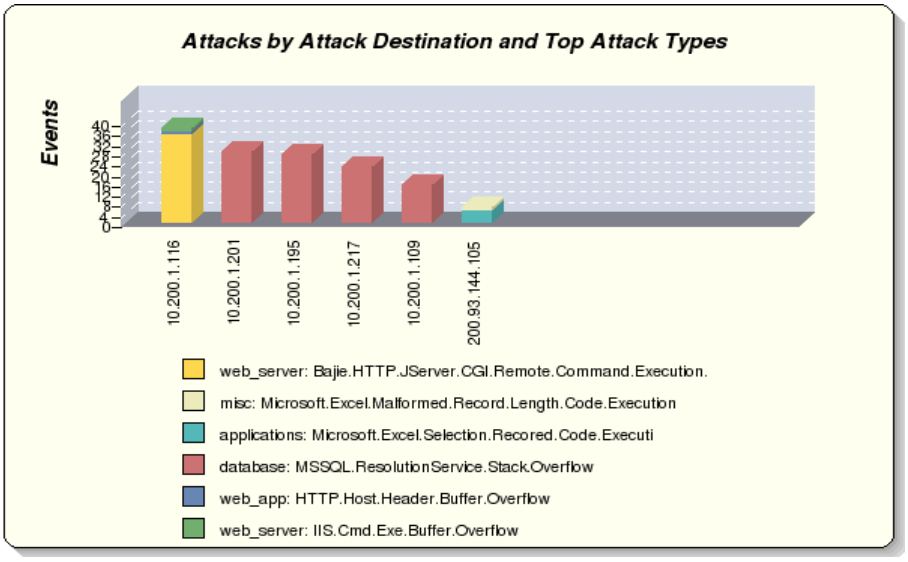


Figura 7. 12 Destino y tipo de ataques

Tabla 7. 5 Destino de los ataques

Destino	Número de eventos
Acuario	37
DNS1	28
Equipo prueba	27
Fortianalyzer	22
Atlantis	15
200.93.144.105	6
Other (43)	59
Total	**194**

Quince: Es importante verificar que los monitores de los servicios conocen y cumplen con el reglamento y las normas de seguridad establecidas. Un factor importante es verificar el puesto de trabajo, para esto se hicieron visitas esporádicas a los mismos cuando se encontraba para determinar si realmente éstos son bloqueados o deshabilitados. Con esto se tuvo un éxito total ya que todos permanecen bloqueados con las sesiones deshabilitadas. Políticas aplicadas administradores 141 y 142.

Dieciséis: Las políticas contemplan un factor importante y es la contingencia que se puedan prestar a los equipos para esto se realizó pruebas a una estación de trabajo, la cual se reinstalo y se dejo intacta en cuanto sin modificar los permisos y perfiles que los usuarios mantienen. Política aplicada 116.

Diecisiete: Cuando ocurre un daño un factor importante es la documentación que se tiene para restablecer el servicio de la manera más pronta, para esto se confrontó el plan de contingencia que se tiene para la recuperación del DNS que al ser seguido paso a paso permitió establecer y recuperar el servicio de una manera pronta. Política aplicada 102.

Dieciocho: Se realizó pruebas de recuperación de copias de seguridad debido a posibles errores humanos que introdujeron fallas en el servicio Web por el borrado de archivos. Se verificó la rapidez en la restauración de copias de una base de datos, esta fue de seis minutos, lo que permitió retornar al normal funcionamiento en el menor tiempo posible. Política aplicada administradores 56.

8 Anexo recomendaciones para la implementación de las políticas de seguridad y el plan de contingencia en el Centro de Datos

- Una implementación escalonada de todas las políticas de seguridad es algo muy recomendable debido a su magnitud y alcance, para que la implementación de las políticas en el Centro de Datos sea más efectiva, debe realizarse una revisión semestral del grado de implantación de las anteriores, así como de su utilidad y acoplamiento a la fecha de dichas revisiones.

- Con miras a la adopción de una norma internacional de seguridad, es conveniente que antes de su instauración se realice un proceso completo en el cual se puedan identificar las posibles necesidades de seguridad, la importancia de implementar una norma para gestionar de una manera adecuada la información, asimismo determinar el nivel de seguridad el cual se ofrece a los datos y servicios administrados actualmente. Este proceso permite determinar de esta manera las ventajas que trae la aplicación una norma de seguridad y las mejoraras efectivas a los mecanismos empleados actualmente en el Centro de Datos.

- Se recomienda la aplicación de 27001, el cual es un estándar de seguridad de la información que puede ser aplicado, para lograr una certificación internacional. Se tienen otros estándares para gestión de la seguridad de la información como ISO 17799, la cual es un código de buenas prácticas que provee lineamientos y recomendaciones para la gestión de la información, pero no es certificable. ISO 27001 además provee los lineamientos necesarios y por sus características se amolda a cualquier organización, la cual debe tomar las pautas y adaptarlas a sus objetivos.

- Si esta norma no puede ser adquirida, la Universidad puede seguir los lineamientos y recomendaciones de ISO 17799, que es una aproximación muy cercana ISO 27001, la diferencia radica en que no es actualmente certificable, pero igual permite que se implementen los mecanismos para el adecuado manejo de la información.

- Realizar un proceso de difusión y formación a los empleados en la importancia de la seguridad de la información para que ellos puedan identificar la necesidad de implementar un sistema de gestión de seguridad de la información, de tal manera que se pueda enseñar el porqué de proteger los activos de información y el papel fundamental que ellos mismos juegan en la administración y gestión de dichos recursos.

- Para un proceso de implementación de los controles propuestos y definidos en las normas con miras a lograr la certificación, se requiere de un grupo de trabajo que puede continuar siendo conformado los roles ya establecidos para la creación de políticas de seguridad. Puntualizando que es de vital importancia que la parte administrativa haga parte constante y activa de este proceso, obteniendo el máximo rendimiento de las soluciones planteadas y asimismo ayudando a disminuir los tiempos en la toma decisiones. Es importante que se tenga la aceptación y el apoyo por parte de la administración de tal manera que pueda cumplir con todos los objetivos planteados.

- Para realizar las actividades que abran las puertas para una posible certificación se debe establecer un horizonte de tiempo, establecer un tiempo de un año y medio para la realización de estos procesos es prudente, ya que realizarlos en un tiempo menor puede acarrear costos los cuales no se pueden asumir y realizarlos en un tiempo mayor puede significar que los controles y mecanismos propuestos se vuelvan obsoletos.

- ISO 27001 propone y tiene como objetivo fundamental la implementación de un SGSI, del cual debe ser capaz de garantizar la confidencialidad, integridad y disponibilidad de la información, asimismo hace especial énfasis en la gestión y análisis de riesgos y en la implementación de controles y políticas para llevar a cabo este proceso. La implementación del sistema puede realizarse de manera manual o automática, para esto se recomienda generar mecanismos o herramientas que permitan hacer los procesos de manera automática.

- Para la implementación del SGSI se recomienda tener en cuenta la documentación del presente trabajo de grado, en aspectos fundamentales como el análisis de riesgos

e implementación de políticas de seguridad de la información y el plan de contingencia.

- La implementación de controles de seguridad se puede realizar por etapas de tal manera que se cubren los principales controles que hacen frente a situaciones y protegen los servicios y servidores de posibles eventualidades, por ejemplo se recomienda emplear las que conciernen a los equipos y servicios y posteriormente se pueden implementar las que conciernen a los usuarios como tal.

- Para el proceso de difusión y formalización de las políticas emplear distintos medios de comunicación tanto escritos como electrónicos tales como la página Web, los correos electrónicos o los medios escritos, adicionalmente realizar jornadas de difusión para dar a entender la importancia de la implementación de controles de seguridad de la información de tal manera que los usuarios y los responsables de la información y los servicios estén totalmente enterados de la importancia de seguridad y el papel que desempeña en la efectividad de los mismos.

- Realizar procesos de revisiones mensuales o trimestrales de tal manera que se puede verificar la metodología propuesta por la norma, la cual pretende que siempre se encuentre en un proceso de mejora continua, revisando los procesos que se han tenido.

- Es conveniente que los procesos se realicen de manera sistemática y controlada, definiendo puntos de partida y elementos de evaluación por ejemplo un caso inicial puede ser el Centro de Datos en la parte concerniente a servidores y servicios, para continuar en un proceso posterior con la infraestructura de red y así posteriormente abarcar de manera completa la división de sistemas en las áreas encargadas de manejar y administrar los sistemas esenciales para administración, cubriendo de esta manera todos los sistemas de información.

- Debido a los altos costos que sugiere la implementación completa de un sitio de réplica de todos los servidores, no es muy factible su implementación en un corto plazo, sin embargo puede irse conformando poco a poco incluyendo nuevos equipos con vista a cubrir estas necesidades en los presupuestos anuales que se manejen

para las compras del Centro de Datos. Pensando en que las nuevas y mejores adquisiciones entren a operar en modo principal, pudiéndose quedar sus reemplazos como las replicas necesarias para instalar en lo posible un sitio en caliente que sería la mejor solución en caso de un desastre natural que afecte gravemente todo el Centro de Datos y cuya magnitud no permita o sea infructuoso la puesta en marcha del plan de contingencia aquí establecido.

9 Glosario

FTP: File Transfer Protocol. Protocolo para la transferencia de archivos.

HTTP: HyperText Transfer Protocol. Protocolo para transferencia de hipertexto.

IMAP: Internet Message Access Protocol. Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

POP: Post Office Protocol. Protocolo de oficina de correo.

SMTP: Simple Mail Transfer Protocol. Protocolo simple de transferencia de correo electrónico.

SSH: Secure Shell. Protocolo de red que facilita las conexiones seguras entre dos sistemas utilizando una arquitectura cliente/servidor.

Vsftp: Very Secure FTP. Muy seguro FTP.

Openssh: versión libre de ssh.

DHCP: Dynamic Host Configuration Protocol. Protocolo de configuración dinámica de equipos.

Scponly: shell restringida que permite unos pocos comandos predefinidos.

Openldap: Open source implementation of the Lightweight Directory Access Protocol (LDAP). Versión libre del protocolo ligero para acceder al servicio de directorio.

Squid: proxy-cache de Internet.

Tsclient: Terminal Server Client. Interfaz que sirve para acceder a escritorios remotos.

IIS: Internet Information Server. Servidor de información de Internet.

Apache: Nombre de la aplicación para implementar un servidor Web.

Icecast2: Sistema de difusión de audio en Internet.

Sarg: Distribución de Linux Debian.

Freeradius: Free Remote Authentication Dial-In user Server. Versión libre del protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

Awstats: Herramienta de código abierto para reportes de análisis Web.

Mrtg: Multi Router Traffic Grapher. Generador de tráfico para gráficos de multi enrutador.

Netflow: Herramienta de monitorización de ancho de banda con soporte Web.

Webalizer: Es un pequeño programa hecho en C el cual que permite generar reportes de alguna página web.

DNS: Domain Name Server. Servidor de nombres de dominio.

Postfix: Servidor de correo. Agente de transporte de correo de código abierto.

Java: Lenguaje de programación orientado a objetos.

Mysql: Sistema de código abierto de gestión de bases de datos.

Jakarta-tomcat: Funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en Apache.

Hosting: Alojamiento sitios Web.

Cisco Pix: Firewall físico fabricado por Cisco.

IPtables: Herramienta Firewall que permite filtrado de paquetes y traducciones de direcciones de red.

10 Bibliografía

[1] Sitio oficial español ISO 27000, http://www.iso27000.es

[2] ISO 27001, pdf ANÁLISIS DE ISO-27001 Seguridad Informatica.pdf. Documento disponible en: http://www.segu-info.com.ar/terceros/terceros.htm

[3] PDCA, página Web disponible en: http://www.iso27000.es/doc_sgsi_all.htm

[4] SGSI, página Web disponible en: http://www.bsispain.com/SeguridadInformacion/ImplantacionSGSI/index.xalter

[5] Control de registros SGSI, pdf ISO27001-norma-e-implantacion-SGSI.pdf. Documento disponible en: http://pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001.doc

[6] Auditorías internas, página Web disponible en: http://iso9001-iso27001-gestion.blogspot.com/2006/11/auditoria-interna-de-un-sgsi-segun-iso.html

[7] Explicación ISO 17799, página Web disponible en: http://www.computersecuritynow.com/presentation/sld002.htm

[8] Norma ISO 15335, doc_otros_estandar_all.pdf. Documento disponible en: http://iso27000.es/download/doc_otros_estandar_all.pdf

[9] Norma ISO 15408, página Web disponible en: http://www.iso.org

[10] Norma ISO 21827, página Web disponible en: http://www.iso.org

[11] BS 7799, Gestion BS 7799.pdf. Documento disponible en: http://www.bsi-global.com

[12] Ley FISMA, página Web disponible en: http://csrc.nist.gov/sec-cert/

[13] Ley FIPS, página Web disponible en: http://csrc.nist.gov/cryptval/140-2.htm

[14] Ley Sarbanex-oxley, página Web disponible en: http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm

[15] Herramienta COBIT, página Web disponible en: http://www.ilustrados.com/publicaciones/EpyFApuplFBpaGVIjY.php

[16] RFC 2196, página Web disponible en: http://www.ietf.org/rfc/rfc2196.txt

[17] Manual de protección IT, página Web disponible en: http://www.blacksheepnetworks.com/security/info/misc/gshb/b/11.htm

[18] OECD, PDF disponible en: http://www.cio.gv.at/securenetworks/oecd/oecd-guidelines.pdf

[19] ISO 15408, página Web disponible en: http://www.iso15408.net/

[20] Rainbow Series, página Web disponible en: http://www.fas.org/irp/nsa/rainbow.htm

[21] ITSEC, página Web disponible en: http://www.itsec.gov.uk

[22] Método CMM, página Web disponible en: http://www.sei.cmu.edu/cmm/cmms/cmms.html

[23] Método SSE-CMM, página Web disponible en: http://www.sse-cmm.org

[24] ISO 11131, página Web disponible en: http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=19150

[25] ISO 13569, página Web disponible en: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37245

[26] Proyecto SOMAP, página Web disponible en: http://www.somap.org

[27] MAGERIT metodología para la gestión y análisis de riesgos de Europa, pagina Web y documentación disponible en: http://www.magerit.es

[28] ACE THREAT ANALISYS AND MODELING herramienta de análisis de riesgos de Microsoft, pagina Web disponible en: http://www.microsoft.com

[29] TRIKE PDF disponible en: http://www.octotrike.org/Trike_v1_Methodology_Document-draft.pdf

[31] PTA, página Web disponible en: http://www.ptatechnologies.com/

[32] Inventario de herramientas y metodologías de ENISA pagina Web disponible en www.enisa.europa.eu/rmra/rm_home.html

[32] Ebios herramienta software para gestión de la seguridad de la información. www.enisa.europa.eu/rmra/methods_tools/t_ebios.html

[33] EAR entorno de análisis de riesgos www.enisa.europa.eu/rmra/rm_home.html

[34] Riskwacth http://www.riskwatch.com/

[35] Callio http://www.enisa.europa.eu/rmra/methods_tools/t_callio.html

[36] Casis http://www.enisa.europa.eu/rmra/methods_tools/t_casis.html

[37] Cobra http://www.enisa.europa.eu/rmra/methods_tools/t_cobra.html

[38] Counter Measures http://www.enisa.europa.eu/rmra/methods_tools/t_countermeasures.html

[39] Cramm http://www.enisa.europa.eu/rmra/methods_tools/t_cramm.html

[42] Proteus, página Web disponible en: http://www.infogov.co.uk/proteus_enterprise/index.php

[43] RA2 pagina Web disponible en: http://www.aexis.de/RA2ToolPage.htm

[44] SOBF, página Web disponible en: http://www.somap.org/sobf/

[47] Documento de Análisis y Modelado de amenazas por Daniel P.F a.k.a metalat/dothacktimes.com pagina Web disponible en: http://metal.hacktimes.com/files/Analisis-y-Modelado-de-Amenazas.pdf