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

Trabajo de Grado

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

LISTA DE FIGURAS

LISTA DE TABLAS

ACRÓNIMOS

ISO: Internacional Standard Organization. Organización Internacional de Estandarización.

BSI: British Standards Institution. Institución Británica de Estandarización.

ICONTEC: Instituto Colombiano de Emisión de Normas Técnicas.

IEC: International Electrotechnical Comisión. Comisión Internacional Electrotécnica.

UKAS: United Kingdom Accreditation Services: Servicio de Acreditación del Reino Unido.

ENAC: Entidad Nacional de Acreditación.

AB: Accreditation Bodies: Entidades de Acreditación.

SGSI: Sistema para Gestión de Seguridad de la Información.

AENOR: Asociación Española de Certificación y Normalización.

FISMA: Federal Information Security Management Act. Ley federal de la Gestión de la Seguridad de la Información.

OECD: Guidelines for the Security of Information Systems and Networks. Directrices para la seguridad de la información de sistemas y redes.

PDCA: Plan-Do-Check-Act. Planear, hacer, verificar y actuar.

IPET: Instituto de Postgrados de Electrónica y Telecomunicaciones.

UPS: Unit Power Supply. Unidad de respaldo para proveer potencia a equipos eléctricos y electrónicos.

SSI: Servidores y Servicios de Internet.

DHCP: Protocolo para la asignación dinámica de direcciones.

FTP: Protocolo para transferencia de archivos.

TIC: Tecnologías de Información y Comunicación.

COBIT: Control Objectives for Information and related Technology. Objetivos de control para la información y tecnología relacionada.

ISACA: Information Systems Audit and Control Association. Asociación de sistemas de información de auditoría y control.

BC/DR: Business Continuity/Disaster Recovery. Continuidad del negocio/recuperación ante el desastre.

RESUMEN

Debido a la importancia que tiene la información, la manera como ésta se gestiona y la tendencia actual de la implementación de nuevos servicios y sistemas que hacen uso de las redes de telecomunicaciones y de los centros de datos, cada día es más importante y necesario garantizar altos niveles de seguridad de la información que permitan la continuidad de los servicios prestados, para esto es necesario adoptar y aplicar estándares y políticas de seguridad de la información que permitan cumplir con los requerimientos mínimos para garantizar seguridad y confianza a los usuarios que hacen uso de los recursos de red y los servicios.

El presente trabajo de grado realiza un estudio y organización de los principales estándares y normas relacionadas con la gestión de la seguridad de la información, como lo son ISO 17799 e ISO 27001, con el fin de orientar la aplicación de alguno para un entorno educativo, para este caso el Centro de Datos de la Universidad del Cauca, que se encarga de garantizar la seguridad de la información del núcleo de la infraestructura de red y de los servicios de Internet que se tienen.

Como paso inicial para implementar los controles y políticas de seguridad para el Centro de Datos, se realizó un estudio y recopilación de las normas de seguridad que por sus características pueden ser aplicadas a este entorno educativo, posteriormente se realizó un análisis de riesgos informáticos, proceso que es muy importante ya que permite determinar y clasificar los elementos que son más importantes tales como servicios, datos, equipos, instalaciones, aplicaciones y el personal, teniendo esta información se enumeraron los que son factibles de ser alterados por una situación inesperada y con esto establecer los criterios para definir las políticas de seguridad y los controles que contribuyen a la meta de brindar mayor seguridad a la información, de igual manera los criterios necesarios para la elaboración de un plan de contingencia que sea capaz de afrontar situaciones de emergencia para restablecer la prestación de los servicios.

INTRODUCCIÓN

Con el establecimiento de políticas de seguridad, el plan de contingencia y el análisis de riesgos informáticos para el Centro de Datos, se logra ofrecer un mayor nivel de calidad en la prestación de los servicios, garantizando seguridad, confidencialidad e integridad de la información administrada. Así mismo el desarrollo y establecimiento de las anteriores procesos es un inicio que abre las puertas para pensar en certificarse en las normas de seguridad de la información establecidas y aceptadas internacionalmente, principalmente la ISO 27001.

Es importante determinar que el proyecto abarca el Centro de Datos de la Universidad del Cauca, es decir el área encargada de los servidores que se tienen para dar acceso a Internet y brindar los servicios para la comunidad educativa, se inició este proceso tomando como punto de partida esta área debido a su importancia, de acuerdo a los resultados obtenidos y la viabilidad de implementar estos controles la Red de Datos pretende en un próximo proyecto replicar estos procesos en áreas como la de infraestructura, desarrollo Web y las encargadas de la parte administrativa.

Para el desarrollo de cada una de las fases se tuvó en cuenta el enfoque del trabajo el cual estaba dado a una institución educativa, en la cual los servicios que se prestan están enfocados a dar el mejor servicio a la comunidad universitaria, conformada principalmente por estudiantes y docentes quienes son las personas que usan al máximo los recursos.

En el desarrollo de este proceso se contó con el apoyo total de las personas encargadas de la administración de los servicios y servidores, quienes permitieron el acceso a la información y a los equipos, un factor importante que influyó en la obtención de la información y en conocer el ambiente de trabajo fue la experiencia que se tenía como trabajadores de esta área.

1. Generalidades de las normas para la seguridad de la información

Antes de introducirse a las normas para la seguridad de la información, es importante tener claros ciertos conceptos que contribuyen a lograr un mejor entendimiento de la temática, para esto se definen aspectos como:

1.1 Política de seguridad

Se puede definir como un conjunto de lineamientos con los cuales se logra mantener un orden y una sistematización. La información que se encuentra contenida en dichas políticas describe o responde a muchos de los procesos o actividades de una organización, las políticas tienen consignadas las acciones que se deben y no se deben tomar, una característica importante es que deben ser accesibles a las personas encargadas de la administración y la gestión de la seguridad. [1]

Una política de seguridad está compuesta por muchos elementos que describen en detalle aspectos importantes tales como los mostrados en la figura 1.1, creada con la utilidad gráfica de *Word*:

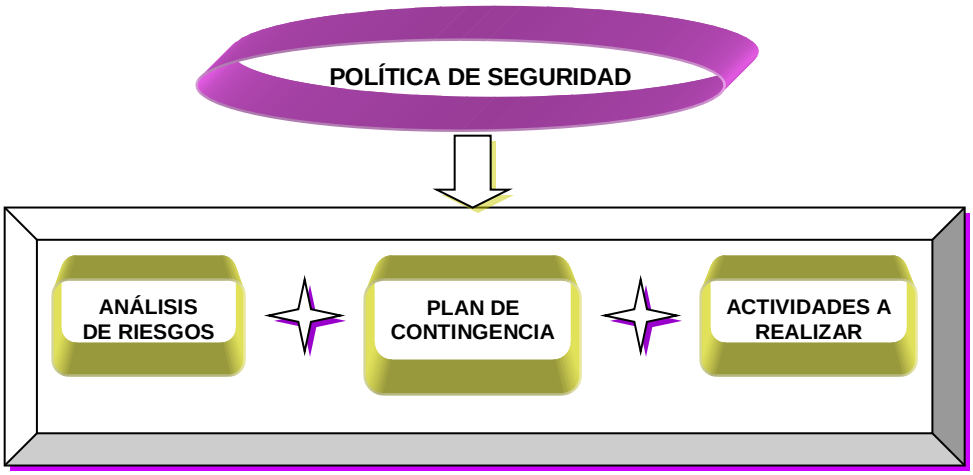


Figura 1. 1 Elementos de una política de seguridad

- Detalles profundos y concretos de posibles riesgos y peligros a los que se encuentra expuesta la organización.

- Plan de contingencia, elaborado para proteger la organización en situaciones de riesgo, especificando de manera clara y detallada los pasos a seguir.
- La manera de actuar de la organización frente a posibles situaciones anormales que ponen en riesgo la continuidad del negocio, en este campo no solo son los correctivos o soluciones técnicas sino también se deben tener en cuenta los correctivos y normas legales.

Una política de seguridad la define, diseña e implementa cada organización de acuerdo a sus características propias, por lo cual es poco probable que pueda comprar un conjunto de políticas de seguridad, aunque existen algunas estandarizadas internacionalmente con las cuales se debe cumplir, se sugiere que la organización tome estos lineamientos, emplee los que son necesarios y adapte y diseñe sus propias políticas para cumplir con los requerimientos y exigencias puntuales de forma que su institución funcione de la mejor manera. Dichas políticas son importantes para una organización, ya que al mantenerlas y cumplirlas se garantiza que la administración y gestión de la información se está realizando de una manera adecuada, garantizando confidencialidad, integridad y disponibilidad.

Entre las ventajas de implementar políticas de seguridad se tiene:

- Generan un factor clave de diferenciación para las empresas, ya que tener las políticas diseñadas e implementadas demuestra que la empresa trabaja y esta lista para atender situaciones anormales, lo que refleja el grado de compromiso que tiene con sus clientes.
- Cumplir con estándares internacionales como los generados por la ISO para el diseño e implementación de políticas y normas de seguridad permite tener un alto grado de calificación a las empresas cuando se realizan auditorías y cuando se siguen procesos de certificación.
- Es útil para actuar en situaciones en donde se ha violado la integridad de la empresa, cuando ocurren delitos informáticos que afectan el normal funcionamiento y la continuidad del negocio, así mismo establece un piso legal en el cual ampararse en estas situaciones inesperadas y que comprometen la integridad de la información.

Dentro de las políticas de seguridad que se pueden encontrar en una organización se tienen diferentes tipos, algunos de los cuales se encuentran en la tabla 1.1 [2]:

Tabla 1. 1 Tipos de políticas de seguridad

Política	Ejemplo
Para el uso de los recursos del sistema.	Establecer horarios laborales y no laborales para permitir el uso de diferentes aplicaciones, de tal forma que aplicaciones que consumen gran ancho de banda no funcionen en horarios laborales.
Para la asignación de cuentas de usuarios.	Para la asignación de una cuenta de usuario se debe diligenciar previamente un formato con todos los datos del usuario, en donde acepte las condiciones de uso de la cuenta.
De copias de seguridad.	Se deben realizar copias diarias de la información de los servicios que los usuarios utilizan con mayor frecuencia y mantener dichas copias en lugares remotos.
De accesos y permisos.	Ningún usuario puede acceder a archivos que no sean de su propiedad.
De seguridad física.	Los equipos se deben mantener en ambientes seguros, lejos de humedades, peligros inminentes de incendios y demás que puedan causarles daño.
Plan de continuidad del negocio.	Se debe diseñar y mantener actualizado un plan de continuidad del negocio.
De alta disponibilidad y redundancia.	Los equipos principales deben contar con equipos replicas que puedan soportar su funcionalidad cuando se presenten fallos.
De monitorización.	Emplear herramientas para gestión de los servicios que se prestan, de tal manera que se puedan generar reportes de su funcionamiento.
De prevención y detección de virus.	Todos los equipos deben contar con mecanismos de protección como los antivirus.
Para el control de accesos remotos.	Los accesos remotos a los equipos deben ser habilitados solo a equipos y usuarios conocidos.
De educación y capacitación en el ámbito de la seguridad.	Todo el personal relacionado con los sistemas debe recibir capacitación sobre la seguridad de la información.
De seguridad perimetral interna en los sistemas informáticos.	Se debe mantener segmentada la red de tal forma que la información crítica se encuentre separada de la información de acceso público.
Para el establecimiento de contraseñas.	Crear contraseñas de mínimo ocho caracteres que incluyan elementos numéricos y alfanuméricos.
Para el cifrado de la información.	Utilizar medios seguros para el transporte y envío del correo electrónico.
Para garantizar la protección de la información.	Establecer los permisos necesarios a los archivos de tal manera que solo los propietarios de dicha información la puedan acceder y modificar.
Para la gestión de los recursos informáticos con los que se cuenta.	Emplear herramientas de gestión de tal manera que se pueda generar reportes de la utilización y acceso a los servicios prestados al público en general.
Legales, de acuerdo a la legislación que cubre el negocio y el país.	Verificar que el manejo de la información no vaya en contra de los derechos personales de los usuarios y empleados.
De control de accesos, definiendo claramente los distintos lugares que se tienen y el acceso a dichos lugares	Restricción de acceso a personal no autorizado a las instalaciones en horarios no laborales.

1.2 Seguridad de la información

Como los demás activos de toda organización, la información constituye un activo de gran valor que debe ser protegido, aplicar controles para la seguridad de la información disminuye el número de amenazas y minimiza los posibles daños garantizando una continuidad del negocio, independiente de la forma de presentación de la información (impresa en papel, imágenes, almacenada electrónicamente o la expuesta en una conversación) esta debe ser protegida adecuadamente. [3]

La seguridad de la información tiene tres aspectos que deben ser preservados para garantizar un adecuado manejo de la información, mostrados en la figura 1.2 creada con la utilidad gráfica de *Word*:

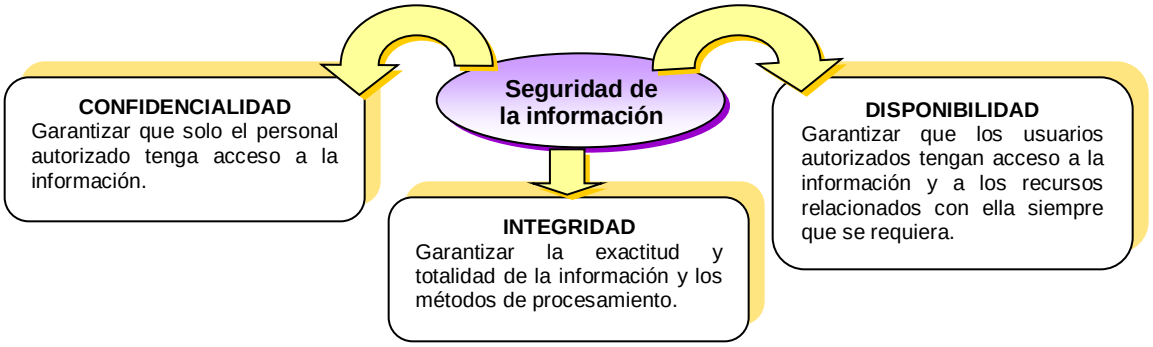


Figura 1. 2 Aspectos claves seguridad de la información

1.2.1 Necesidad de seguridad de la información

La información, los procesos, sistemas y redes que dan apoyo a una organización constituyen importantes recursos, la dependencia de la organización respecto a estos sistemas de apoyo denota que es más vulnerable a las amenazas concernientes a la seguridad de estos elementos, ya que se enfrentan continuamente y en forma creciente con amenazas de diversos orígenes, como el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación, daños como los realizados mediante ataques con virus informáticos, "*hacking*[1]" y denegación de servicio. La confidencialidad, integridad y disponibilidad de la información se vuelven esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la

[1] Hacking: es la técnica o arte de encontrar los límites de los productos, aparatos y servicios digitales de informática o comunicaciones y compartirlo con otros y/o los fabricantes mismos de ésos productos.

imagen comercial. Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada, por lo cual debe ser respaldada por una gestión y procedimientos adecuados. [3].

1.2.2 Certificación en seguridad de la información

Es un proceso que le permite a una organización ser reconocida por el cumplimiento de estándares establecidos internacionalmente, esta certificación garantiza que una empresa cuenta con los lineamientos que se han propuesto y especificado bajo las directrices de una organización internacionalmente aceptada y reconocida, como la ISO y la BSI. Una certificación en general, asegura la calidad y emite cierto respaldo o garantiza que una entidad, un producto o una persona está cumpliendo con los estándares mínimos dentro de los que se miden y califican ciertos parámetros de seguridad.[4]

1.2.3 Proceso de certificación

Para que una empresa pueda acceder al proceso de certificación según la BSI, se deben cumplir y seguir ciertos lineamientos que aseguran una efectiva implantación del sistema de gestión de la seguridad. Para esto se han establecido seis pasos. Figura 1.3, creada con la herramienta gráfica de *Word:* [5]

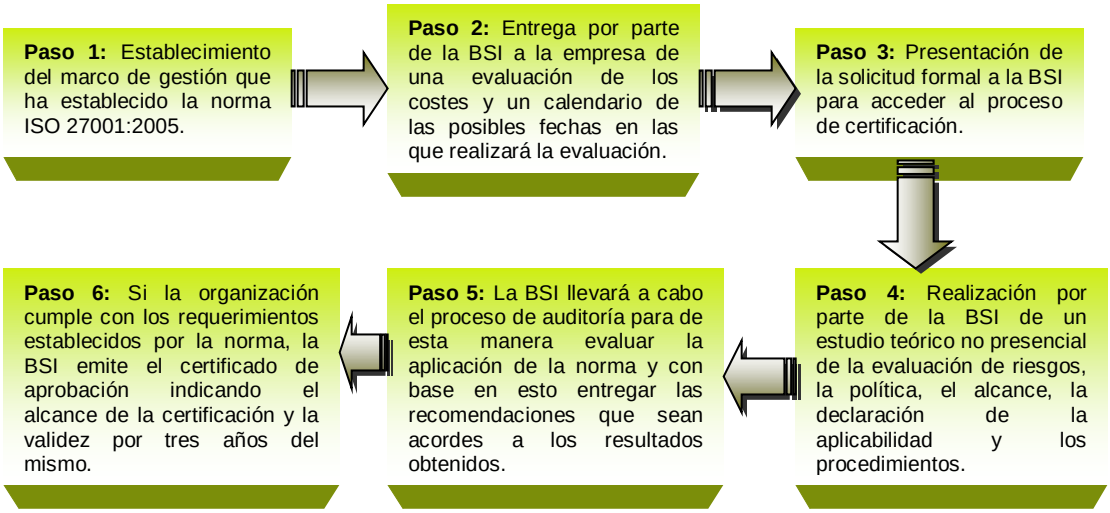


Figura 1. 3 Pasos para la certificación

Según ICONTEC para Colombia cuando una empresa desea acceder a un proceso de certificación debe seguir las etapas mostradas en la figura 1.4, creada con la *Word:* [6]

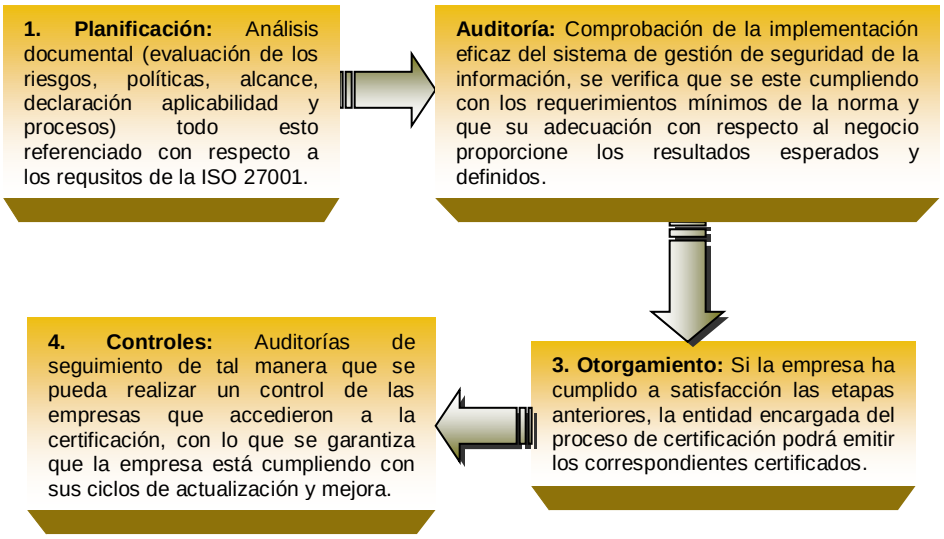


Figura 1. 4 Procesos de certificación en Colombia

1.2.4 Entidades que pueden realizar un proceso de certificación

Actualmente se cuenta con dos entidades internacionalmente establecidas y reconocidas que son la ISO y la BSI, estas entidades son las de mayor jerarquía que emiten las normas y tienen la autoridad para emitir certificaciones y para acreditar y homologar empresas para que puedan realizar este proceso, así mismo cada país cuenta con empresas de estandarización para normas, las cuales deben estar homologados por alguna de las entidades para que el certificado que emite tenga valides en el ámbito nacional e internacional. Para Colombia se tiene ICONTEC. [7]

- **ISO:** Entidad responsable para la normalización a nivel mundial, conformada hasta la fecha por 130 países que a su vez está constituida por comités técnicos, cada uno de los cuales es responsable de la normalización para cada área de especialidad. Es un órgano consultivo de las Naciones Unidas y coopera estrechamente con la IEC, que es responsable de la estandarización de equipos eléctricos. Su propósito es promover el desarrollo de la normalización para fomentar a nivel internacional el intercambio de bienes y servicios, para el desarrollo de la cooperación en

actividades económicas, intelectuales, científicas y tecnológicas. El resultado se publica en forma final como normas internacionales. [8]

- **BSI:** Es la primera entidad de normalización mundial de origen inglés, es un instituto reconocido el cual trabaja bajo el estudio de la UKAS en el Reino Unido, ENAC en España y por la AB, que son empresas acreditas para ofrecer servicios de certificación de un SGSI. Actualmente entre las entidades certificadoras solo BSI dispone de un sistema para homologar a consultores asociados para la implementación de BS 7799-2:2002. [9]
- **ICONTEC:** Instituto Colombiano de Normas Técnicas y Certificación. Es la entidad encargada de certificar las normas de calidad y certificación de empresas y trabajos. También se encarga de ciertas normas de presentación de trabajos y cartas hechas en computador o cualquier otro medio. [6]

1.2.5 Beneficios de la certificación en seguridad de la información

Los beneficios indiscutiblemente son muchos, independiente de lograr o no una certificación al implantar normas y políticas de seguridad de la información que garanticen confidencialidad, integridad y disponibilidad de la misma, se logra que la gestión y administración de los activos y los recursos con los que cuenta la organización sea más ordenada y eficiente, además que permite mantener planes de continuidad del negocio para actuar frente a posibles eventualidades que interrumpan el constante funcionamiento. Otros beneficios adicionales que se obtienen al lograr que una empresa se certifique son: [10]

- Incrementa el nivel de conciencia del personal con respecto a los temas de seguridad informática, ya que los informa de los posibles riesgos a los que están expuestos, así mismo de las posibles consecuencias que se pueden derivar de estos.
- Permite que el sistema de gestión de la información se adapte a las características del negocio de tal manera que permita un uso eficiente y un desempeño adecuado, además que sea compatible con otros sistemas de gestión como lo son el de calidad y el medioambiental.

- Contar con la certificación proporciona una ventaja que marca la diferencia en el mercado lo cual se retribuye en un mejor posicionamiento del negocio, así como la proyección de una imagen que para el usuario final genera una sensación de tranquilidad y satisfacción, además que estar certificado garantiza calidad y transparencia.

1.2.6 Factores críticos del éxito

Los siguientes son algunos de los factores que pueden resultar críticos a la hora de realizar la implementación de la seguridad de la información en una organización, por lo que se debe velar por su adecuada implementación: [11]

- Política de seguridad, objetivos y actividades que reflejan y enmarcan las características y elementos importantes de la empresa.
- Una estrategia de implementación de seguridad de la información que sea consecuente con los procesos y organización administrativa de la empresa.
- Apoyo y compromiso manifiestos por parte de la gerencia (su análogo de la parte administrativa).
- Comunicación eficaz de los temas de seguridad a todo el personal encargado de la administración y a los empleados.
- Distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas.
- Instrucción y entrenamiento adecuados referentes a la implementación de controles y mecanismos de seguridad.
- Un claro entendimiento de los requerimientos de seguridad y la administración y evaluación de riesgos.
- Un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a la mejora de los mecanismos empleados.

1.2.7 Algunas entidades auditoras

Actualmente solo BSI entre las entidades certificadoras dispone de un sistema para homologar a consultores asociados para la implementación de la norma ISO 27001. Estas empresas consultoras especializadas en seguridad informática y en sistemas de la información tienen el objetivo de realizar el trabajo previo necesario para la adecuación en los clientes finales interesados en obtener una certificación ISO 27001, en la tabla 1.2 se muestra algunas de las empresas auditoras de Europa homologadas por la BSI y que ofrecen sus servicios a nivel internacional:

Tabla 1. 2 Empresas auditoras de Europa.

Empresa	Descripción
Nextel	Actúa como consultora en la implantación de sistemas de gestión de la seguridad de la información basados en ISO 27001. La primera empresa de España con un SGSI certificado por BSI y la única con dos certificaciones, al contar con la certificación UNE 71502 de AENOR. En Junio de 2006 ya disponía de la certificación ISO 27001 por migración administrativa. [12]
Applus+	Compañía de certificación de carácter global con presencia en más de 25 países y más de 25 sectores en expansión, representa la unidad de negocio del grupo Agbar[2] y tiene como misión convertirse en un referente internacional en el negocio de la certificación.[13]

1.2.8 Algunas entidades certificadas

En el año 2006, 3.274 organizaciones fueron certificadas en el mundo en la norma ISO 27001 y BS 7799-2. En ISO 27001 son exactamente 669, cifra que incluye 267 actualizaciones de certificaciones desde BS 7799-2:2002 y 402 nuevas certificaciones. Encabeza la lista como desde hace años, Japón, con 1.850 certificaciones, le siguen el Reino Unido con 334 y la India con 290. Una idea del rápido crecimiento que está experimentando la certificación es que, a finales de 2004, eran unas 1000 empresas las que estaban certificadas en todo el mundo y a finales de 2005, unas 2.100.

Los países de habla hispana que aparecen en la lista, con su número de certificaciones, son: México con 11, España con 9, Argentina con 3, Colombia con 2, Chile, Perú y Uruguay con 1. [14]. La figura 1.5 creada con la herramienta gráfica de *Word*, muestra algunas de las empresas certificadas:

[2] Agbar: Consorcio de más de 230 empresas y 140 años de historia.

- Telefónica Empresas CTC Chile, certificación en BS 7799-2:2002
- Telefónica Soluciones de Informática y Comunicaciones de españa, S.A. Sociedad Unipersonal.

De Colombia:

- ETEK International Holding Corporation, número de certificado IS 84320, certificación en BS 7799-2:2002.
- UNiSYS Global outsourcing & Infrastructure Services (GOIS)/Maintenance Support Services (MSS), número de certificado IS 97104, certificación en BS 7799-2:2002.

Figura 1. 5 Empresas certificadas en seguridad de la información

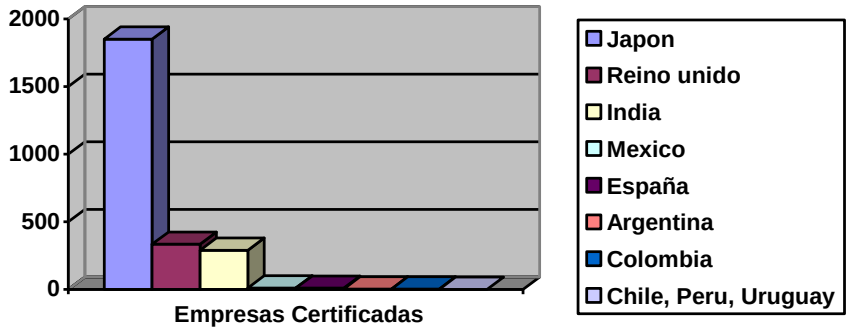


Figura 1. 6 Paises con empresas certificadas en gestión de la seguridad

1.3 Normas para la seguridad de la información

En la tabla 1.3 se enumeran algunas de las normas mas importantes en seguridad de la información, el anexo 1 del presente trabajo de grado contiene información detallada.

Tabla 1. 3 Normas de gestión de seguridad de la información

Nombre	Descripción
ISO 27000	Su objetivo principal radica en la implementación y diseño de un sistema para proveer seguridad de la información, dicho sistema debe permitir preservar la confidencialidad, la integridad, disponibilidad y autenticidad de esta, características que le permiten a los usuarios accederla en el momento que lo requieren, con la seguridad de que esta completa y manejada de una forma segura. [15]
ISO 27001	Este estándar fue desarrollado principalmente para dar los lineamientos que permitan a una empresa implementar un SGSI, de tal manera que dicha empresa sea autónoma y capaz de mantener los lineamientos y pautas que le permitan diseñar, implementar, mantener, revisar y monitorizar su propio sistema. Permite a cada empresa adecuarlo a su necesidad de negocio, de manera que la complejidad del sistema depende del negocio en si. Una característica fundamental está en que la norma está orientada a lograr que en una organización se mejore la forma como se realiza la gestión de la seguridad de la información [16].
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 administración 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 conocida como Código de buenas Prácticas [17].
Norma 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. [18]

Tabla 1. 4 Normas complementarias para gestión de seguridad de la información

Nombre	Descripción
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. [19]
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. [20]
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 la norma BS 7799-2 bajo el esquema de mejoramiento continuo del ciclo PDCA. [21]
FISMA	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 gobierno electrónico, las empresas que tengan la responsabilidad de manejar las TI, o información que es relevante, 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. [22]
FIPS 140-2 Ley Estadounidense	Estándar 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. [23]
Ley Sarbanes-oxley	Es una ley estadounidense que 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 perdida 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. [24]
COBIT	Esta basada en un conjunto de normas globales que permiten realizar una administración y gestión de una manera centralizada y organizada. [25]
RFC 2196	La IETF elaboró este RFC denominado Site security handbook, este documento es una guía para los administradores de equipos y servicios que se ofrecen en Internet, ya que ofrece lineamientos y recomendaciones que pueden ser tenidas en cuenta para aplicar los elementos y correctivos necesarios para asegurar un tratamiento adecuado de la información. [26]
Manual de protección IT	Genera los lineamientos básicos para la protección de la información, este documento presenta métricas o recomendaciones para la implementación de safeguards o medidas de control que ayuden a minimizar los riesgos a los cuales encuentran expuestos los elementos que constituyen los sistemas información. Es desarrollado por la agencia de información de Alemania y es denominado baseline protecction manual. [27]
OECD	La OECD 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. [28]

Tabla 1. 5 Estándares para evaluación de seguridad en sistemas

Estándares para evaluación de seguridad en sistemas	
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 computadores para comprobar si un determinado producto cumple tales requisitos. [29]
ITSEC Reino Unido.	Es un documento que desarrolló el Reino Unido, se basa en los parámetros recomendados por el TSEC, aunque los desarrolló con mayor profundidad un documento muy útil ya que a la recomendaciones es el uréter información que ser tenidas en cuenta. [30]
La serie arco iris Rainbow Series (ornage 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 resultar importantes libros, los más conocidos es el *trusted computer system evaluation criteria* (TSEC o orange book), en cuales un documento útil para la gestión de su información. [31]

Tabla 1. 6 Estándares para desarrollar aplicaciones

Estándares para desarrollar	
CMM.	El instituto e ingeniería lidero el desarrollo de este método de cuales muy importante ya que cuenta con aspectos de seguridad que deben ser tratados en proyectos de desarrollo en seguridad de la información. [32]
SSE-CMM.	Es un derivado de la anterior norma. [33]

Tabla 1. 7 Estándares para servicios financieros

Estándares para servicios financieros	
ISO 11131.	Es un estandar para servicios financieros, especialmente hace enfasis en los del sector bancario en aspectos claves como los tipos de autenticación que se pueden manejar. [34]
ISO 13569.	Lineamientos para la seguridad de información en servicios financieros. Este estándar proveer lineamientos para políticas, organización y estructuras así como mecanismos y regulaciones legales y consideraciones para la selección implementación de controles de seguridad. Este estándar no es de libre distribución y debe ser adquirido. [35]

Comparación entre estándares y definición del que servirá de guía para el desarrollo de las políticas y controles para el Centro de Datos

Para el desarrollo de los lineamientos propuestos en el presente trabajo de grado, con el fin de garantizar y generar los procedimientos de seguridad que mejor se acoplen al Centro de Datos, así como después de realizar el proceso de análisis y conocimiento de algunas de las normas más importantes que actualmente se tienen establecidas a nivel internacional, se determinó: es muy importante para este proceso basarse en un estándar

y una norma internacional, debido a que actualmente Colombia no ha generado un estándar o una norma para la gestión de la seguridad de la información, el ICONTEC que es el instituto que regula esta normatividad a optado por introducir y aceptar el estándar de la norma ISO 27001. Del proceso realizado previamente se encontró que la norma ISO 27001 genera unos lineamientos que se requieren para la gestión de la seguridad de la información, esta norma es actualmente certificable y guarda una correspondencia directa con la norma ISO 17799, la cual también genera las directrices y lineamientos necesarios para la gestión de la seguridad de la información, no es certificable y se distribuye con el fin de generar las recomendaciones para ir generando los mecanismos para la implementación de la norma ISO 27001. Para el entorno educativo y los procesos que se quieran realizar dicha norma genera las recomendaciones necesarias para que dicho proceso pueda llevarse a cabo de una manera muy completa.

Junto a la norma ISO 17799 mencionada anteriormente también se ha optado por tomar como base los lineamientos dados en el RFC 2196 que se complementan de una manera adecuada y permiten realizar los procesos de una manera ágil. Por tal motivo para realizar los procesos de análisis de riesgos e implementación de controles y planes de contingencia se tomará como base las recomendaciones de la norma ISO 17799 y el RFC 2196 abriendo de esta manera los primeros procesos para que en un futuro el Centro de Datos de la Universidad del Cauca pueda iniciar un proceso de certificación en la norma ISO 27001. Las normas complementarias o desarrolladas para la legislación y los procedimientos de otros países sirven de aporte y de complemento en este proceso pero no son tomados como base para llevarlas a cabo, en la tabla 1.8 se puede observar algunas de las características analizadas en este proceso.

Tabla 1. 8 Comparación entre estándares de seguridad de la información

Nombre	Estándar internacional	Certificable en gestión de seguridad de la información	Descripción
ISO 27001	SI	SI	Estándar internacional para certificación en gestión de la seguridad de la información.
ISO 17799	SI	NO	Estándar internacional que provee lineamientos para gestión de seguridad de la información.
ISO 11131	SI	NO	Provee lineamientos para el sector bancario de los Estados Unidos.
ISO 13335	SI	NO	Es una guía con un compendio de documentos de seguridad para tecnologías de la información.
FIPS 140-2	NO	NO	Lineamientos para el desarrollo de software

			criptográfico.
BS7799	SI	SI	Estándar británico para certificación en gestión de la seguridad de la información.
COBIT	SI	NO	Conjunto de lineamientos de buenas prácticas para seguridad de la información.
SARBANES-OXLEY	NO	NO	Ley de seguridad de la información para las empresas estadounidenses.
RFC2196	SI	NO	Conjunto de recomendaciones para la seguridad de la información.
FISMA	NO	NO	Ley estadounidense para seguridad de la información.
ITIL	SI	NO	Biblioteca de recomendaciones para seguridad de la información.

2. Análisis de riesgos para el Centro de Datos

Este capítulo contiene el desarrollo del análisis de riesgos realizado al Centro de Datos de la Universidad del Cauca, para su realización se emplearon los lineamientos propuestos por los estándares de seguridad y en especial por la metodología Magerit, para información adicional de procesos de análisis de riesgos refererirse al anexo 2 en la parte de riesgos informáticos. Este desarrollo se encuentra dividido en dos partes, una inicial que comprende la fase de planificación y estructuración del análisis de riesgos, es decir, en esta parte se encuentran contenidos los informes referentes a los recursos, distribución del personal, identificación del entorno, la definición y descripción de objetivos, la segunda parte contiene información fruto de la recolección y el análisis de datos en lo concerniente a elementos importantes tales como: servicios ofrecidos, datos e información relevante a amenazas y medidas de protección con las que cuenta.

Parte 1 informes del proyecto

2.1 Informe preliminar estudio de la oportunidad

Es importante la realización de un análisis de riesgos para el Centro de Datos de la Universidad del Cauca, ya que permite definir y determinar como es el estado del riesgo y el nivel de seguridad que actualmente se tiene, así mismo obtener una base firme y sólida sobre la cual se pueden obtener y determinar las necesidades básicas y los requerimientos mínimos para garantizar un adecuado funcionamiento. El desarrollo del proceso trae consigo grandes beneficios y genera las bases para que la Universidad pueda en un futuro ingresar en un proceso de certificación en seguridad de la información como el establecido por la norma ISO 27001, de esta manera puede obtener un posicionamiento y reconocimiento a nivel nacional e internacional, además, ser pionera en ese tipo de procesos y en la apropiación de esta temática.

Los resultados del análisis de riesgos realizado al Centro de Datos proporcionan las bases para que el proceso de gestión de la seguridad de la información se pueda realizar

de una manera adecuada y eficaz, además de la sensibilización y el reconocimiento por parte de los administradores de los servicios y servidores de la necesidad de la realización de estos procesos para llegar a implementar políticas de seguridad que puedan ayudar a mejorar las actividades y procesos que actualmente se realizan.

En cuanto a necesidades de seguridad que se tienen actualmente se pueden enumerar las más trascendentales y que han dado origen a este proyecto:

- Cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas, las cuales se pueden encontrar en el documento de controles y políticas de seguridad existentes en el Centro de Datos que se encontrará como documento confidencial en el área de servidores y servicios de Internet de la Red de Datos.
- Se requieren controles más fuertes para los problemas de seguridad que se pueden presentar, ya que no se contemplan y es necesario brindar niveles superiores de seguridad.
- Es conveniente establecer y definir los activos de información, para tener una visión clara y precisa de la importancia de los elementos con los que se cuenta.

2.1.1 Conformación de los comités y el grupo de trabajo

De acuerdo a lo recomendado por la guía metodológica general, debido a la complejidad y alcance que pueden incluir las políticas, se conforma un grupo de trabajo para su diseño, grupo en el que se incluyó al personal que se relaciona directamente con el Centro de Datos de la universidad. Los roles asumidos se pueden observar en la tabla 2.1:

Tabla 2. 1 Comites y grupo de trabajo

Nombre	Integrantes	Funciones
Comite de dirección.	• Administrador del área de servicios y servidores de Internet de la Red de Datos. • Jefe de la División de Sistemas.	• Su función principal es aprobar los resultados de cada proceso a ser aplicados al Centro de Datos. Otra función es revisar la posibilidad de asignar recursos y medios necesarios para la ejecución del proceso de análisis de riesgos.
Comité de seguimiento.	• Administrador del área de servicios y servidores de Internet de la Red de Datos. • Docente departamento de Sistemas del programa de	• Las responsabilidades de este grupo de personas se enmarcan durante este proceso en la solución de posibles inconvenientes que pudieran retrasar la consecución de resultados y la aprobación de los informes generados durante éste análisis, además de

	Ingeniería Electrónica y Telecomunicaciones.	asegurar que se cuente con los medios necesarios y la disponibilidad de los mismos para que las personas encargadas de este proceso de análisis de riesgos lo puedan realizar.
Equipo de desarrollo.	• Fabián Andrés Mera y Carolina Guevara Campo, estudiantes del programa en Ingeniería Electrónica y Telecomunicaciones.	• Llevar a cabo las tareas necesarias para revisar el proceso de análisis de riesgos. • Recopilar, procesar y consolidar información y datos que permitan llevar a buen término el proceso. • Elaborar los informes requeridos y necesarios que se vayan generando durante el desarrollo del proyecto.

2.1.2 Aproximación inicial del análisis de riesgos.

La Universidad del Cauca actualmente cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas, tampoco cuenta con planes de contingencia que permitan afrontar posibles situaciones de riesgo para su Centro de Datos, actualmente presta servicios muy importantes que necesitan ser atendidos de una manera eficaz y que debe garantizar el adecuado nivel de seguridad.

Algunos servicios esenciales que se soportan en el Centro de Datos son los servicios canónicos o principales de Internet, considerados criticos, se enumeran en la tabla 2.2:

Tabla 2. 2 Servicios ofrecidos en el Centro de Datos

Servicio	Descripción Servicio
Web , hosting	Por medio de este la Universidad cuenta con su propio portal en Internet, además permite a los grupos de investigación, las facultades y las dependencias contar con un espacio para alojar sus propios portales y aplicaciones.
Navegación Proxy	Permite a los usuarios de Unicauca acceder a Internet.
FTP	Este servicio es brindado a la comunidad universitaria en general para mantener información y aplicaciones que son necesarios para la formación académica.
E-mail	Se cuenta con dos servidores de correo, que cubren y dan soporte a los estudiantes, docentes y el personal que hace parte de Unicauca.
Bases de Datos	Es de carácter interno y solo pueden acceder las aplicaciones que hacen uso del *hosting* de Unicauca.
DNS	Servidor de Nombres de dominio, el cual es la base de la navegación y es muy importante para el funcionamiento de los otros servicios
Administración de Ancho de Banda	Permite darles diferentes prioridades a las aplicaciones y garantizar un determinado ancho de banda según requiera las aplicaciones y el perfil de usuario.
Detección de Spam	Actualmente se cuenta con un sistema para detección que trata de reducir en gran medida la cantidad de correo no deseado.
Streaming	Aplicación para la difusión a través de Internet de la emisora de la Universidad del Cauca.
Acceso remoto (RAS)	Para permitir que los usuarios de la Universidad puedan acceder desde sus casas a Internet empleando línea telefónica.
Asignación dinámica de direcciones	Con el DHCP se asigna de una manera dinámica direcciones a los usuarios, de tal manera que ya no es necesario realizar configuraciones manuales por parte de los usuarios y los administradores.

Servicio de Directorio LDAP	Mantiene un registro centralizado de los usuarios que acceden a las aplicaciones y servicios ofrecidos, permitiendo la autenticación y validación de estos usuarios.
Direcciones públicas y NAT	Para los usuarios que requieran acceso a Internet con aplicaciones especiales se les ofrece el servicio de asignación de direcciones reales, o el servicio de NAT global con el fin de que puedan hacer uso de estos servicios.

2.1.3 Servicios fundamentales que ofrece

En la figura 2.1, creada con *Word*, se encuentran referenciados algunos de los servicios más importantes y los cuales son percibidos y empleados con mayor frecuencia por los usuarios.

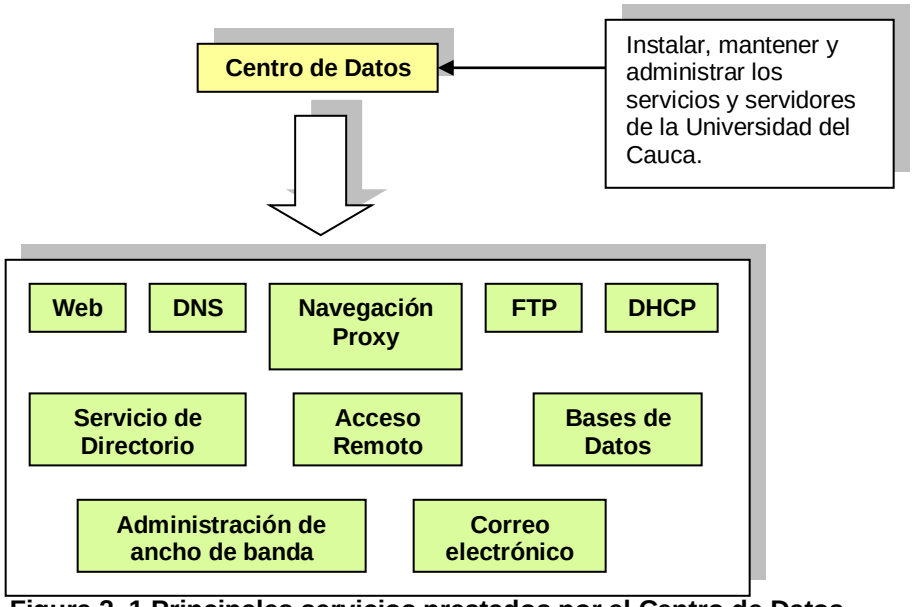


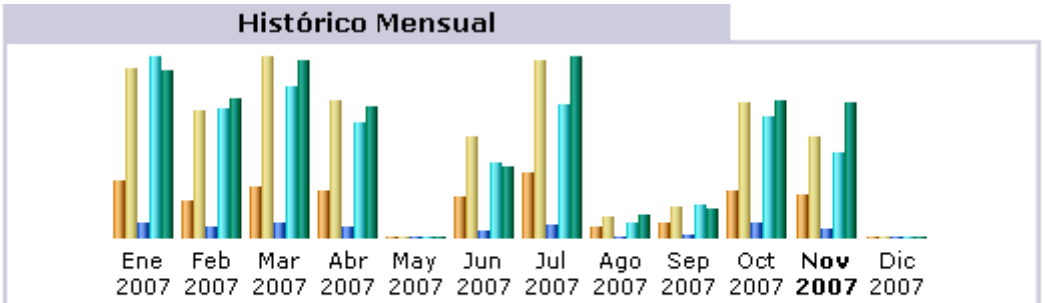
Figura 2. 1 Principales servicios prestados por el Centro de Datos

Es importante destacar que los servicios ofrecidos están funcionando de una manera óptima y están aprovechando sus recursos de manera eficiente, lo que no quiere decir que no se deba realizar una análisis de riesgos previo de tal manera que se puedan mejorar los procesos actuales y se puedan ofrecer servicios de calidad que cumplan con los requerimientos de seguridad tal como lo exigen los estándares, además que este proceso abre las puertas para que en un futuro se pueda pensar en una posible certificación en seguridad de la información con la ISO 27001.

2.1.4 Estadísticas de uso de los servicios y servidores

Esta parte del proceso se realizó con la colaboración de las personas encargadas de

administración y gestión de los servicios del Centro de Datos y la infraestructura de red, estos datos corresponden a valores aproximados que son obtenidos con las aplicaciones que analizan los archivos de sucesos de los servicios y de los equipos, aplicaciones como Awstat, Nagios e información sumistrada por el personal. Las gráficas que se tienen son como las mostradas en la figura 2.2 la cual corresponde al histórico del acceso al servicio Web que mantiene el portal de la Universidad, obtenido con la herramienta *webalizer*.



Mes	Visitantes distintos	Número de visitas	Páginas	Solicitudes	Tráfico
Ene 2007	31282	94283	721802	8586316	35.71 GB
Feb 2007	20682	70155	551325	6109339	29.63 GB
Mar 2007	28562	100205	679695	7246500	37.98 GB
Abr 2007	25783	76800	562826	5452652	27.98 GB
May 2007	756	873	3411	48327	183.32 MB
Jun 2007	22891	56556	305932	3612662	14.95 GB
Jul 2007	36508	98931	660522	6320499	38.41 GB
Ago 2007	6192	11677	73883	760954	4.77 GB
Sep 2007	8842	17678	153384	1561855	6.40 GB
Oct 2007	26498	74903	728353	5798798	29.44 GB
Nov 2007	23820	56487	396665	4053668	28.66 GB
Dic 2007	0	0	0	0	0
Total	231816	658548	4837798	49551570	254.11 GB

Figura 2. 2 Grafica de análisis del servicio Web de www.unicauca.edu.co

Asimismo se tienen una serie de estadísticas para los servicios que requieren mayor disponibilidad debido a los usuarios que los acceden, por el tipo información que manejan. La cantidad de accesos y trafico que ha circulado en lo corrido del ultimo año se consigna en la tabla 2.3, se puede observar la cantidad de visitas de usuarios externos e internos que hacen uso de los servicios soportados, la cantidad de tráfico y de visitas que se tienen es considerablemente alto, ya que éstos son los equipos que soportan los servicios esenciales que son la cara visible de las aplicaciones hacia Internet.

Tabla 2. 3 Uso del servicio Web

Descripción	Odin	Afrodita	Atenea	Acuario
Numero de visitas externas	102293	2099552	3255455	231816
Numero de visitas Totales	130406	2941524	4602095	658548
Paginas visitadas	271210	10761560	13325706	4833798
Total de solicitudes	272909	10761560	13325706	49551570
Total de tráfico	1247, 88 Gb	192, 78 Gb	30, 29 Gb	254, 11 Gb

Actualmente se cuenta con dos servidores de correo, uno destinado para manejar los correos de docentes y administrativos, otro para manejar los correos de estudiantes, en la tabla 2.4 se puede observar un aproximado de la cantidad de correos que se han manejado en lo corrido del año, donde se puede notar que el volumen de información que se maneja es muy alto, lo que sustenta la importancia de este servicio.

Tabla 2. 4 Correos enviados en los servidores del Centro de Datos

Descripción	Atenea		Afrodita	
	Numero	Tamaño	Numero	Tamaño
Correos enviados y recibidos con éxito	1`623.842	41.29 Gb	1`531.688	25.57 Gb
Correos rechazados	84.693	970.51 Mb	52.704	470. 90 Mb

El tráfico promedio que manejan diariamente los dos proxys se puede observar en la tabla 2.5. Esta información fue obtenida con el programa Iptraf, el cual es un analizador de trafico que se encuentra instalado en los equipos proxy.

Tabla 2. 5 Porcentaje de uso de los servidores proxy

Proxys	Total interfaz ethernet	Total interfaz ethernet
Temis	16539 kbps	2720 paquetes
Hiperion	14359 kbps	2210 paquetes

Por la capacidad de los enlaces hacia Internet, en la tabla 2.6 se puede observar el promedio de su ocupación en horas comprendidas entre 9 -11 am y 2-5 pm en dias laborales. Para obtener esta información se empleó el programa MRTG que es un sistema de monitorización para los enlaces que actualmente maneja el Centro de Datos, los porcentajes de uso de los enlaces fueron suministrados por el historico que ofrece la herramienta, en la figura 2.3 se puede observar la capacidad de uno de los enlaces de Internet durante una semana del mes de diciembre de 2007, el cual es monitorizado con MRTG, donde se observa una capacidad promedio de 8 Mbps.

Tabla 2. 6 Porcentaje de uso de los enlaces de Internet

Enlaces	Promedio Hora pico kbp/s		Promedio diario kbp/s		Promedio Mensual kbp/s	
	IN	OUT	IN	OUT	IN	OUT
EMTEL	4137. 9	1792. 5	2122. 7	7045.8	5938. 3	3264. 6
ETB	4088. 4	528. 7	241. 6	10. 7	2789. 9	259. 4

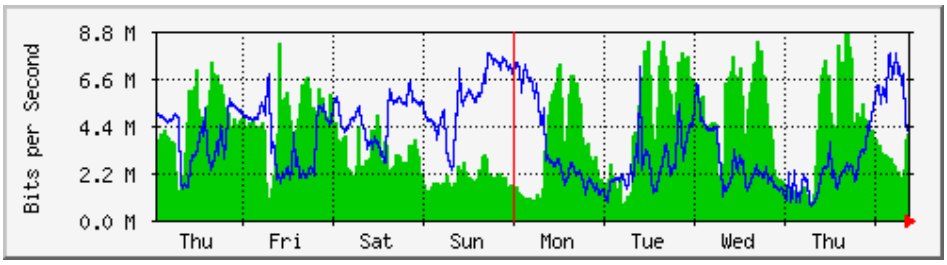


Figura 2. 3 Gráfica del enlace de EMTEL de la Universidad del Cauca

Para la monitorización de los servicios y equipos utiliza la herramienta Nagios, la cual permite gestionar los servicios y mantener un control del estado de los servicios y del estado de los equipos, como se puede observar en la tabla 2.7:

Tabla 2. 7 Equipos gestionados con Nagios

Nombre de los equipos	Descripción
Acuario, Afrodita, Atenea, Cronos, Dns1, Dns2, Fortianalyzer, Fortigate, Gestionservidores, Hades, Hera, Híperion, Temis, Juno, Netenforcer, Netexplorer, Odin, Perseo.	Servidores del Centro de Datos.
Core4507, stodomingo, ingenierias, recursos, financiera, matematicas.	Equipos de red.
HTTP, FTP, SSH, SMTP, POP, IMAP, DNS, LDAP, PROXY, DHCP, PING.	Servicios Soportados en los servidores.

El número de usuarios que al mes de diciembre de 2007 se encuentran registrados para hacer uso de los servicios que ofrece como el correo electrónico, cuentas en el servidor Web y el FTP se encuentran en la tabla 2.8:

Tabla 2. 8 Usuarios registrados en las aplicaciones del Centro de Datos

Nombre	Número de usuarios registrados	Descripción
Red cableada.	2800	Computadores que actualmente se encuentran habilitados para acceder a recursos de la red.
Red Inalámbrica.	74	Computadores que actualmente se encuentran habilitados para hacer uso de los recursos de la red inalámbrica.
Usuarios Acuario.	292	Corresponde a los sitios web que se encuentran alojados y pertenecen a facultades o grupos de investigación.
Usuarios Atenea.	3090	Usuarios del correo electrónico.
Usuarios Afrodita.	8227	Usuarios del correo electrónico.

Usuarios Odin.	38	Corresponde a las cuentas de usuario para administrar información en el FTP.

Tabla 2. 9 Tipos de usuarios de Atenea

Tipos de usuario	Numero
Grupos de investigación	90
Contratistas	79
Dependecias	180
Docentes	1041
Funcionarios	586
Grupo de Actividades	113
Pensionados	13
Eventos	52
Especiales	111

Con las estadísticas del uso de los servicios y recursos del Centro de Datos se complementa y se justifica la información obtenida de referencia que determina la importancia de los servicios canónicos o fundamentales de Internet, como lo son el correo electrónico, el servidor Web, el servidor FTP y los servidores Proxy, de esto no se puede olvidar que éstos servicios a su vez requieren de otros servicios como el DNS, LDAP, que son fundamentales para poder prestar su funcionalidad.

2.1.5 Medios para realizar el proceso

El proceso se realizará, como parte inicial del proyecto de grado “Criterios para establecer políticas de seguridad: caso de estudio Centro de Datos de la Universidad del Cauca”. Por lo cual todos los medios materiales, de tipo logístico, humano, etc, son aportados y considerados por el desarrollo de este trabajo de grado.

2.2 Informe fase de planificación

2.2.1 Objetivos:

- Identificar si el Centro de Datos de la Universidad del Cauca tiene problemas que comprometan la seguridad de la información almacenada en los servidores, mantenida por los servicios, aplicaciones, posibles deficiencias en la gestión y administración de recursos.
- Analizar actualmente las principales necesidades y riesgos de seguridad del

Centro de Datos de la Universidad del Cauca.

- Identificar los principales elementos que hacen parte del Centro de Datos, determinando servicios, datos, aplicaciones software, hardware, personal e infraestructura.
- Estimar y determinar las posibles riesgos y amenazas a las cuales se encuentra expuesto el Centro de Datos.

2.2.2 Restricciones generales

El análisis de riesgos del Centro de Datos de la Universidad del Cauca, es parte de un trabajo de grado, su finalidad es generar los documentos necesarios que puedan dar los lineamientos básicos que servirán para formular recomendaciones y mejorar los métodos y mecanismos que se tienen para la gestión de seguridad de la información. Debido a su alcance se presentan algunas restricciones que se mencionan a continuación:

- **Temporales:** el análisis de riesgos debe ser realizado en un tiempo corto no mayor a un mes, ya que por el calendario del trabajo propuesto es el tiempo estimado para este proceso.
- **Políticas o gerenciales:** en este Ítem la parte administrativa desempeña un papel importante, ya que el resultado de dicho análisis puede llevar a consideraciones que en un futuro sirvan para la implementación de metodologías y estándares para gestión de riesgos.
- **Metodológicas:** se empleará la metodología en cascada muy similar a la propuesta por el plan PDCA. No se puede emplear en esta fase una metodología en espiral, ya que las condiciones de tiempo no lo permiten.
- **Personal:** se cuenta exclusivamente con dos estudiantes los cuales se encargarán de realizar el proyecto.
- **Confidencialidad:** la información generada de este proyecto esta sujeta a la revisión y aprobación del administrador del Centro de Datos, quien determinará que tipo de información puede ser publicada y cual debe ser tratada de manera confidencial.

2.2.3 Determinación del alcance del proyecto

El análisis de riesgo se realizará al Centro de Datos de la Universidad del Cauca donde se tiene el núcleo de la infraestructura de red y los equipos que soportan los servicios esenciales para las actividades de la comunidad universitaria, se realizará a los servicios esenciales y a los equipos de red e informáticos que permiten que dichos servicios se puedan prestar. El Centro de Datos se encuentra ubicado en el IPET, en este lugar se encuentran alojados los equipos de red y los servidores que permiten prestar a la comunidad universitaria los servicios esenciales para llevar a cabo muchas de sus actividades cotidianas.

- **Determinación de los límites**

El dominio de trabajo es el Centro de Datos de la Universidad del Cauca, el cual se encuentra conformado por la sala de servidores, ubicada en el Instituto de Postgrados del programa Ingeniería Electrónica y Telecomunicaciones. El análisis abarcará los servicios esenciales y la determinación del nivel de riesgo de seguridad a los cuales se encuentran expuestos los servicios y servidores.

Identificación del entorno

Las áreas que contemplan los servicios de Internet se pueden determinar por:

- Los equipos de red que permiten ofrecer la conectividad necesaria para acceder a Internet.
- Los equipos y el software empleado para garantizar la seguridad de los equipos tanto al interior de la Universidad como fuera de ella.
- Los equipos físicos que alojan las aplicaciones que permiten prestar los servicios.
- Las aplicaciones que soporta, para el monitoreo de la información y la prestación de servicios.
- Las estrategias y los medios de gestión y administración de la seguridad de la información para los servicios esenciales que actualmente se tienen.

Las funciones del área encargada de la administración del Centro de Datos

Las funciones corresponden a las necesarias para garantizar que los equipos de red y servidores presenten un adecuado funcionamiento, asimismo que los usuarios finales puedan hacer uso de los servicios ofrecidos por la Universidad de una manera eficaz y con niveles de calidad aceptables. Dentro de estas funciones podemos definir labores más puntuales:

- Instalación y configuración de equipos de red y servidores.
- Configuración de los servicios con los que cuenta.
- Mantenimiento de los servicios y aplicaciones.
- Mejoras a los servicios y equipos.
- Atención a las necesidades por demanda que requieren los usuarios.
- Estudio e implementación de mecanismos de seguridad.

El Centro de Datos se constituye en el pilar fundamental de la Red de Datos de la Universidad del Cauca, ya que es el núcleo desde el cual se prestan todos los servicios, por esto cualquier falla en el mismo ocasiona grandes traumatismos para la red de la Universidad, por tal motivo se determina que la relación y dependencia con las otras áreas funcionales es muy alta, lo que le da mucha importancia, además se encarga de mantener los equipos y los servicios que ofrece a la comunidad universitaria, así mismo debe ofrecer servicios de atención y asesoría a los usuarios pertenecientes a esta red universitaria que requieren el uso de los sistemas y aplicaciones que aquí se tienen en funcionamiento.

2.2.4 Definición de grupos de usuarios que se ven afectados en el proceso

Los servicios que ofrece son empleados por diferentes tipos de usuarios, algunos de estos usuarios tienen control sobre ciertas aplicaciones y servicios, pero dicho control es limitado y regulado. Los diferentes usuarios se encuentran consignados en la tabla 2.10

Tabla 2. 10 Usuarios del Centro de Datos

Usuarios	Descripción
Jefe de área.	Quien es el encargado de tomar decisiones que conciernen a la administración, mejora, planeación, diseño y cambios de los servidores, servicios de red y aplicaciones.
Administradores del Centro de Datos.	Monitores que tienen funciones de administración, control y monitoreo sobre todos los servidores y los servicios ofrecidos.
Los administradores de aplicaciones.	Soportados sobre los servidores y el espacio Web, base de datos y aplicaciones informáticas y equipos.
Usuario de servicios y aplicaciones.	Conformado por docentes, estudiantes y administrativos quienes pueden hacer uso de la información pública que es almacenada en estos servidores y los servicios en general.

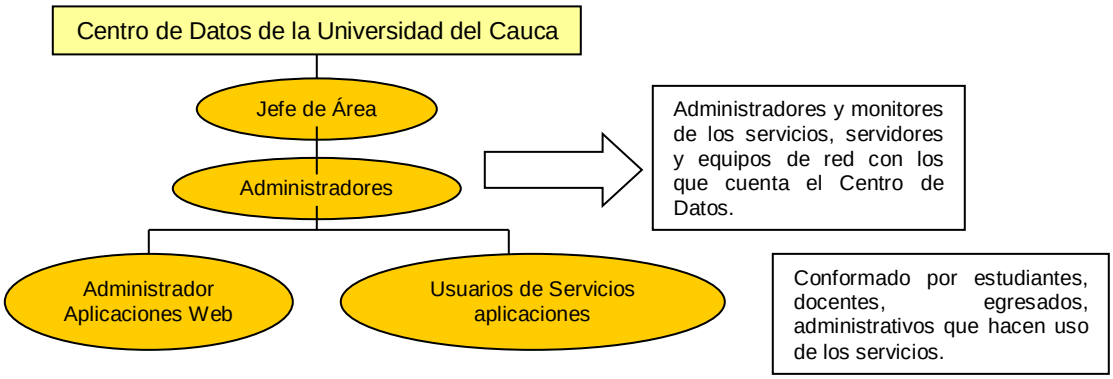


Figura 2. 4 Organigrama del Centro de Datos

2.2.5 Plan de entrevistas para recolección de información

Las entrevistas se realizarán al administrador del Centro de Datos, a los estudiantes que desempeñan el rol de monitores del área de servicios y servidores de Internet, quienes realizan las tareas de administración de servidores y servicios del Centro de Datos, las preguntas que se realizaron se encuentran consignadas en el anexo tres.

2.2.6 Cargas de trabajo

El proyecto se realizará por dos estudiantes en un tiempo de un mes, el procedimiento consiste en recolectar y analizar información relevante a los servicios, con base en esto realizar un chequeo de la organización y de la información.

2.2.7 Planificación del trabajo

El tiempo para realizar el análisis de riesgos es de un mes. El cronograma de referencia para las actividades se muestra en la figura 2.5:

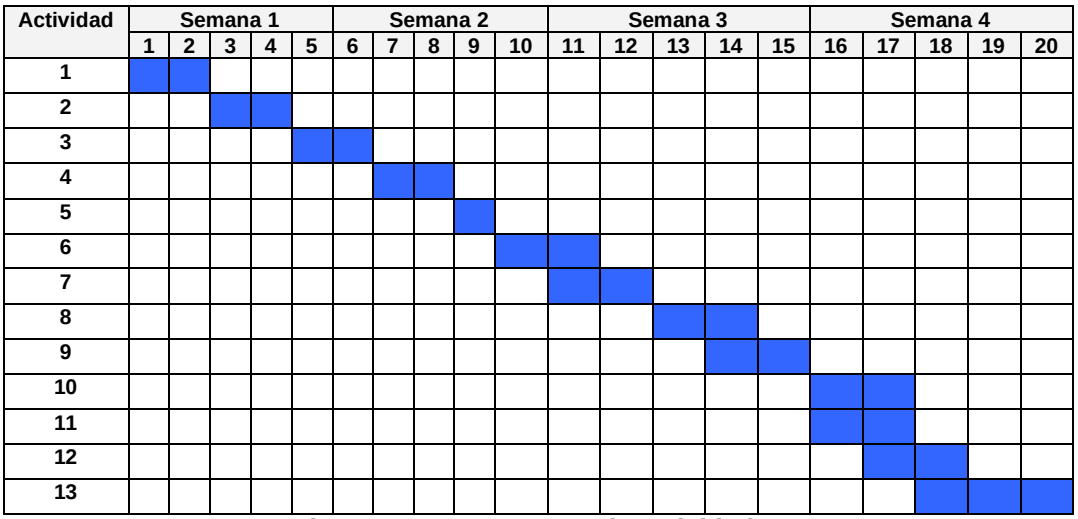


Figura 2. 5 Cronograma de actividades

Tabla 2. 11 Actividades cronograma

Actividad	Descripción
1	Planificación del proyecto.
2	Inicio fase inicial y recolección de información.
3	Entrega del informe Preliminar, el cual llevará la información necesaria para iniciar el proyecto.
4	Puesta en marcha del proyecto.
5	Definición de roles y asignación de responsabilidades.
6	Realización de entrevistas y recolección de información de manera más detallada en lo referente a servicios y equipos de red con los que se cuenta.
7	Realización del informe inicial acerca del estado actual de la seguridad.
8	Definición de activos.
9	Clasificación de activos.
10	Determinación de amenazas
11	Clasificación amenazas.
12	Generación del informe preliminar de análisis de riesgos.
13	Presentación y análisis de resultados

2.2.8 Estimación de costos

El costo aproximado de la realización de este análisis, acorde a las características, los limites y dominio antes planteado se muestra a continuación.

Tabla 2. 12 Recursos hardware

Nombre del hardware	Cantidad	Valor compra	Horas Uso	Justificación	Costo total
Computador Dell Optiplex GX280	2	$3’906.207	160	Equipos terminales	$207.900
Impresora	1	$350.000	10	Imprimir la documentación	$15.167
Total recursos de equipos					$223.067

Tabla 2. 13 Recursos software

Nombre del software	Cantidad	Valor compra	Justificación	Costo total
Linux Debian Sarge 3.1	1	Libre distribución	Sistema operativo para la realización de la documentación.	$0
Opennoffice.org	1	Libre distribución	Paquete software para procesamiento de textos.	$0
Total recursos software				$0

Tabla 2. 14 Recursos de personal

Persona	Semanas trabajo	Horas de trabajo semana	Nº Total de horas	Valor punto	Puntos hora	Costo total
Director	4	2	8	$7676	2.5	$153.520
Codirector	4	2	8	$7676	2.5	$153.520
Estudiante 1	4	40	160	$7676	1.5	$1’842.240
Estudiante 2	4	40	160	$7676	1.5	$1’842.240
Total recursos de personal						$3’991.480

Tabla 2. 15 Recursos bibliográficos

Nombre del software	Cantidad	Valor compra	Justificación	Costo total
Recursos bibliográficos		$150.000	Documentación de Internet, necesaria para el proyecto	$150.000
Total recursos Bibliográficos				$150.000

Tabla 2. 16 Materiales e insumos

Nombre del recurso	Cantidad	Justificación	Valor
Resma de papel tamaño carta	1	Imprimir la documentación	$8.000
Cartucho tinta negra impresora	1	Imprimir la documentación	$7.000
Cartucho tinta color impresora	1	Imprimir la documentación	$7.000
CD´s	4	Para copiar la documentación	$2.000
Encuadernación de documentos		Presentación de informes	$20.000
Materiales de oficina		Necesarios para desarrollar el proyecto	$20.000
Total Materiales e insumos			$64.000

Tabla 2. 17 Total de costos

Rubros	Total
Recursos de personal	$3’991.480
Recursos de Equipos	$223.067
Recursos software	$0
Recursos bibliográficos	$150.000
Materiales e insumos	$64.000
total del proyecto	$4’428.547

2.2.9 Puntos importantes para el inicio del proyecto

De las etapas anteriores se tienen definidos puntos importantes y mecanismos para la recolección de información, de este proceso y los cuestionarios se pueden obtener la información necesaria para el análisis y gestión de riesgos. Estos cuestionarios se realizarán y se adaptarán de acuerdo a las características de funcionamiento y operación del Centro de Datos de la Universidad del Cauca. Es importante tener en cuenta que los cuestionarios deben estar enfocados y desarrollados con respecto a los objetivos planteados, el dominio y el alcance que se han definido y los temas más importantes para que este proceso se pueda llevar a cabo, los cuestionarios identifican los activos, las amenazas, las vulnerabilidades, el impacto del riesgo y las medidas de protección existentes, además de identificar las posibles restricciones que se puedan generar con el desarrollo proyecto. Los cuestionarios se deben adaptar a cada institución educativa, ya que cada una cuenta con una visión y un entorno que puede ser diferente, lo que hace necesario una perspectiva diferente para la recolección de información.

2.2.10 Criterios de evaluación para el proceso de análisis de riesgos

- 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.
- Informe de activos, amenazas y vulnerabilidades.
- Informe con el estudio de los resultados.

Parte 2 Captura de Información

2.3 Informe estado actual de seguridad del Centro de Datos

En términos generales en el tema de seguridad de la información realiza actividades de monitoreo y seguridad que le permiten mantener y prestar un adecuado servicio, dichas actividades son realizadas de manera manual y en la mayoría de las ocasiones no se tiene un registro actualizado de los procedimientos y de las situaciones inesperadas que

pueden surgir.

Actualmente cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas, las cuales se pueden encontrar en el documento de controles y políticas de seguridad existentes en el Centro de Datos que reposará como documento confidencial en el área de servidores y servicios de Internet de la Red de Datos. Para solventar posibles situaciones de anomalías que pongan en riesgo la seguridad de la información, el no tener políticas de seguridad implica que no se tiene referencia de cómo proceder en situaciones de riesgo ni cómo proceder para aplicar los correctivos necesarios. Así mismo no cuenta con personal en el tema de seguridad de la información, que se dedique exclusivamente a proteger y estar al frente de situaciones de riesgo. El trabajo de esta área es realizado de manera alterna por el personal del área encargado de administrar los servidores y servicios de Internet.

El Centro de Datos no se encuentra certificado por alguna entidad internacional reconocida en el tema de seguridad de la información, así mismo no maneja un estándar para el tratamiento de la información, de igual forma no cuenta con un plan de contingencia que permita estar preparado para afrontar una situación de riesgo, estas falencias evidencian la necesidad de la implementación y aplicación de un estándar que permita hacer un uso más eficiente de los medios con los que se cuenta, así mismo uno que proporcione mayor calidad y un servicio que pueda demostrar niveles de seguridad mucho más altos que los actuales.

La Universidad representada en el área de las tecnologías de la información por el Centro de Datos cada día implementa utilidades y aplicaciones que permiten a la comunidad universitaria agilizar procesos, pero también generan e incorporan nuevas brechas de seguridad ya que la masificación de su uso y los nuevos requerimientos en cuanto a hardware y software pueden en ocasiones atentar contra la integridad, disponibilidad y confidencialidad de la información gestionada, brechas a las cuales hay que permanecer atentos para entrar a corregirlas, ejemplos de esto se pueden ver en las nuevas plataformas para administración de contenidos Web las cuales tienen vulnerabilidades que deben ser solucionadas manualmente.

Para realizar este análisis y encontrar las situaciones de riesgos mas influyentes se inicia con una serie de cuestionamientos iníciales, los cuales se han dividido por áreas y el objetivo es recoger información y encontrar el estado real de la seguridad. Este análisis inicial trata de definir los aspectos más importantes que están generando posibles factores de riesgo que al no tenerlos en cuenta pueden generar situaciones inesperadas, el análisis completo se deja como documento confidencial al área de servidores y servicios de Internet.

Inicialmente se empleará como referencia y punto de partida las preguntas realizadas en el anexo tres del presente trabajo de grado, el cual esta basado en las guías propuestas por Nextel S.A[3] para la aproximación inicial de la realización de una auditoria en seguridad. [1]

En una primera instancia conviene saber con que cuenta la Universidad del Cauca, es decir que tipo de mecanismos está empleando para el manejo de la información, siguiendo este orden de ideas es conveniente indagar sobre los siguientes aspectos los cuales se encuntran consignados en las siguientes tablas:

Políticas de Seguridad de la información
• Actualmente cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas para la gestión de la seguridad de la información y los servicios que ofrece a la comunidad universitaria. El personal a cargo maneja métodos de seguridad y mecanismos para garantizar la seguridad de la información y las aplicaciones, pero dichos métodos no se encuentran formulados de una manera formal en un documento en el cual se puedan guiar para realizar estas labores. Actualmente se encuentran establecidas algunas políticas para administración del canal de acceso a Internet y el tipo de tráfico que puede circular y pasar.
• La seguridad de la información y las aplicaciones se encuentra actualizada con respecto a las necesidades actuales de seguridad, pero no se encuentra documentadas o no se realizan con respecto a un proceso definido el cual permita evaluar estos procesos.
• Los usuarios que hacen uso de las aplicaciones soportadas no conocen las reglas y las políticas que se tienen, ya que no se encuentran disponibles o no se ha realizado una campaña informativa para dar a conocer estos lineamientos de tal manera que se apliquen correctamente.

Organización de la seguridad
• El Centro de Datos no cuenta con una persona dedicada exclusivamente al control de la seguridad. Actualmente los administradores de los servicios realizan controles de seguridad para verificar el correcto funcionamiento de las aplicaciones pero no hay lineamientos definidos acerca del tema, por lo tanto esta actividad se realiza por iniciativa propia, o cuando ocurre una situación excepcional.
• Realmente no se realiza una capacitación formal en seguridad de la información, las personas encargadas de la administración se forman con respecto a las necesidades que van surgiendo y lo realizan de una manera autodidacta.

[3] Nextel S.A: Empresa consultora en seguridad de la información.

• Se disponen de algunos controles de seguridad, enfocados a accesos restringido a los servidores, se emplea el Firewall[4] y el servicio para detectar accesos no permitidos del equipo analizador del tráfico para evitar intrusiones desde Internet y mecanismos para evitar caídas de los servicios, pero no se encuentran documentados ni establecido de una manera formal.
• No se mantiene una relación con empresas especialistas en seguridad de la información. Actualmente el Centro de Datos no trabaja con personal capacitado en esta área que le pueda brindar un soporte técnico y operativo.
• Los mecanismos de control de la seguridad que se aplican a los servicios no se tienen documentados, por tal razón cuando se realizan procedimientos, estos no quedan plasmados en un documento.

Control y clasificación de activos
• Al respecto no se tiene definido de manera clara cuales son los elementos de la organización, ni se tiene una clasificación que permita discriminarlos e identificarlos.
• Por ausencia de una clasificación de activos no se puede determinar que activos son más importantes para la organización y cuales se deben proteger de una manera más completa.
• Se mantienen controles sobre los equipos existentes, pero no se encuentran documentados dichos controles y no se mantiene actualizada la documentación de los equipos con respecto a los cambios que han ido surgiendo, aunque se sabe con precisión donde se encuentran, no se tiene por escrito el estado actual.
• No se tienen procesos para realizar o implementar mecanismos de seguridad, ya que dichos procesos no se realizan ni se mantienen por escrito.
• Actualmente el área de servicios de Internet es la responsable de los activos de información que se encuentran alojados y así mismo de los servicios de Internet que se ofrece.
• La seguridad de los activos se supervisa por iniciativa propia y la gestión de los servicios se realiza con tareas programadas, es decir si un servicio falla se debe realizar el análisis para encontrar la posible situación que genera esta anomalía, estos procesos no se encuentran documentados.
• Los usuarios que hacen uso de los servicios, especialmente aquellos que tiene a su cargo la responsabilidad de gestionar o administrar alguna aplicación no son evaluados para determinar si cuentan con la formación necesaria que les permita buscar mecanismos para garantizar la seguridad de la información.
Seguridad del Personal
• En este caso no se cuenta con puestos de trabajo claramente definidos ya que los cuatro monitores realizan las mismas funciones y cuentan con el mismo grado de responsabilidad, a excepción del jefe de área quien toma las decisiones en cuanto a procedimientos que se deben seguir, como variante se asignan tareas puntuales a cada monitor que se deben socializar.
• Realmente las responsabilidades de seguridad se tienen pero no están definidas, por tal razón dichas responsabilidades se han distribuido de igual manera.
• Cada administrador se forma en seguridad de la información de manera autodidacta y conforme los requerimientos de seguridad que van surgiendo.
• El personal que se encuentra a cargo de la administración de los servicios del Centro de Datos cuenta con una clasificación y pasa por un proceso de aceptación en el cual se verifica que cumpla con ciertas características.
• Para la administración de los servicios ofrecidos no se cuenta con personal subcontratado.

Seguridad Física y Ambiental
• Realmente el Centro de Datos no cuenta con mecanismos de seguridad que restrinjan el perímetro, más que el acceso restringido el cual es controlado por una llave, una alarma y un guarda que verifica el acceso.
• En este lugar se encuentran los equipos de red capaces de dar acceso a Internet por medio de los canales contratados, los equipos que soportan la seguridad perimetral y la administración del ancho de banda[5], así mismo el equipo de red principal que es el que da soporte a la intranet y los servidores que soportan los servicios básicos como lo son el servicio WEB, FTP, DNS, PROXY E-

[4] Firewall: Cortafuegos. Equipo de red empleado para ofrecer seguridad a los equipos que hacen parte de una red de área local.
[5] Ancho de banda: capacidad de flujo de datos que se tiene para acceder a Internet.

MAIL, RAS, LDAP, que son fundamentales para la comunidad universitaria.
• Para evitar los cortes de energía se tienen dos circuitos alternos y UPS. Pero actualmente se presentan fallas y su tiempo de carga máximo aproximado oscila alrededor de treinta minutos.
• Los procedimientos de seguridad están determinados por el acceso restringido por llave, no se cuenta con un procedimiento el cual registre quien estuvo en el Centro de Datos a determinadas horas y con que fines.
• Las estaciones de trabajo de los monitores se encuentran ubicadas en una instalación diferente al Centro de Datos, instalaciones a las cuales pueden acceder los otros monitores de la red. Cabe notar que estas estaciones cuentan con contraseñas de acceso restringidas.
• Cuando se mueve un equipo o se daña existen ciertos controles para poderlos instalar en sus nuevas posiciones o localidades. Pero estos informes corresponden al área de equiposa. El área de SSI no lleva un control de estos equipos donde se pueda observar con que equipos se cuenta y cuales han salido de uso.

Tecnologías de información, operaciones y comunicaciones
• Actualmente no cuenta o no sigue un estándar de seguridad de la información, de tal manera que se pueda apuntar hacia una posible certificación en seguridad de la información. En las áreas administrativas o técnicas que cubren las otras operaciones que soporta tampoco se cuenta con ningún tipo de certificación o proceso de certificación.
• No se tienen procesos o mecanismos que puedan hacer frente a posibles cambios que se den dentro de la organización, es decir no se tiene referencia de ningún estándar para actuar frente a posibles cambios en cuanto a estructura o tecnología.
• Existen procedimientos de planificación de software, un mecanismo que utilizan antes de emplear una nueva aplicación informática consiste en implementarlo y dejarlo como prueba algunos días de tal manera que se pueda verificar su funcionamiento, a pesar de esto no existen mecanismos que permitan que el Centro de Datos pueda realizar análisis del software que se va a emplear de manera controlada y que permita generar una documentación posterior.
• Actualmente se realizan copias de seguridad a los correos electrónicos, pero este proceso no se realiza de manera continua, se realiza al correo electrónico de los usuarios y se esta borrando cada ocho días, actualmente se tiene en proceso la implementación de un sistema de backups que permitirá realizar las copias de respaldo de gran parte de la información que se maneja en Unicauca.
Control de accesos
• El acceso a los equipos hardware que prestan soporte para los servicios se encuentra restringido a los administradores y solo se realiza el control de acceso por medio de los archivos de sucesos del sistema, pero a estos archivos no se les realiza un tratamiento de la información que pueda llevar a cabo un registro de control de accesos o un historial de los usuarios que han accedido a los sistemas.
• Para el control de accesos no se cuenta con herramientas de monitorización que permitan realizar este control de manera más dinámica que permitan analizar por parte de los administradores con mayor claridad y que incluso generen alarmas cuando se presente una anomalía.
• Para la asignación de contraseñas a los servidores se cuenta con mecanismos que no se encuentran documentados, las contraseñas deben cumplir con ciertos requerimientos, aunque no se emplean controles para verificar la efectividad de estas. Por otro lado no se han educado los usuarios del sistema para que introduzcan contraseñas que sean difíciles de descifrar, así mismo no se cuenta con mecanismos que las comprueben y las rechacen cuando no cumplan con un nivel o parámetros mínimos de seguridad.
• Los usuarios que hacen uso del servicio de correo electrónico, actualmente para solicitar una cuenta deben demostrar mediante recibo de matricula que se encuentran matriculados, la administración de la contraseña y de la cuenta es responsabilidad del usuario, ya que no se tiene mecanismos para verificar que la contraseña introducida cumple con los niveles de seguridad requeridos, así mismo no se tiene registro diferente al de los registros del sistema para verificar la actividad de los usuarios y no se maneja ningún tipo de caducidad.
• Actualmente no se cuenta con seguridad en el caso de conexión de nuevos equipos o equipos portátiles de tal manera que al introducir un nuevo equipo se registre en la red, dichos equipos se pueden conectar fácilmente a la red y no se puede mantener un control de los mismos, y esto debido en gran parte a la gran cantidad de usuarios que conforman la red universitaria.
• El área de servicios de Internet conoce algunas de las posibles amenazas que podrían afectar el funcionamiento de una manera global, además saben que tan importante es protegerse para

afrontar estas situaciones, pero no las tienen documentadas o clasificadas formalmente, por tal razón en ocasiones se vuelve difícil evitarlas.

Mantenimiento y desarrollo de sistemas
• El área no se encarga de desarrollar nuevas aplicaciones.
• Sobre el servidor Web que es el principal, se implementan nuevas aplicaciones, las cuales antes de ponerlas en funcionamiento se prueban en servidores diferentes o equipos replica para constatar su funcionamiento, así mismo antes de realizar la implementación o mejora de un nuevo servicio, este pasa por una fase de prueba para verificar su comportamiento y mirar las características del mismo.
• Cuando se realizan cambios en los sistemas no se emplean estándares o acuerdos de nivel de servicio, aunque dichos cambios se realizan de una manera planificada al no existir una documentación adecuada no se puede realizar un adecuado seguimiento.
• No se ha realizado un desarrollo para los procesos de control del Centro de Datos, es decir, no se cuenta con una aplicación que permita seguir los procesos de control que requiere el área.
• Sobre los desarrollos que se han implementado sobre los servidores Web no se tiene documentación de tal manera que se pueda retomar el trabajo en un futuro, por una persona diferente al desarrollador original.
• No se emplean procedimiento predictivos para la detección de fallos, de tal manera que se pueda estar preparado frente a posibles situaciones de riesgo que comprometan la integridad de los sistemas. Tampoco se tiene una realimentación de las posibles situaciones o fallos de seguridad de los sistemas ya que no se mantiene una base de datos donde se registren estos eventos.
• El área de servicios de Internet cuenta con muy buenas herramientas de monitorización para verificar el funcionamiento y el estado de las aplicaciones y el ancho de banda que se dispone, de esta manera se esta ofreciendo un servicio de calidad constante.

Planes de continuidad del negocio
• El Centro de Datos no cuenta con una plan de continuidad que permita que en un evento inesperado se puedan emplear procedimientos o mecanismos que permitan que la prestación de los servicios no se vea interrumpida y que se pueda restaurar de una manera eficaz, aunque el área de SSI cuenta con documentación de los servicios que administra, esta documentación se debe actualizar y se debe mejorar ya que se han introducido nuevos servicios.
• No se tiene una plan de continuidad y no se han probado de alguna manera los mecanismos que se tienen para proporcionar o para ayudar que los servicios retomen su funcionamiento de una manera adecuada.
• Así mismo no se tienen políticas para activar el plan de continuidad.

Control de adecuación a las leyes
• Actualmente no cuenta con una herramienta o mecanismo que permita verificar el cumplimiento de la legislación, verificar que esta cumpliendo con estándares y esta proporcionando los niveles de seguridad adecuados.
• No se tienen auditorias externas que permitan verificar el cumplimiento de estos mecanismos.
• Parcialmente se esta informado de los perjuicios relativos al no cumplimiento de la legislación a nivel personal y corporativo, ya que se conocen algunas normas de ley que se deben cumplir y no se deben pasar por alto, se tiene referencia sobre el pago de licencias y el uso de software.
• Los empleados no están completamente informados de sus responsabilidades relativas al cumplimiento de la legislación, es decir son concientes de algunas leyes, pero al no existir formación se pueden incurrir en faltas a esta legislación.

Situaciones inesperadas que afectan el normal funcionamiento y desempeño del Centro de Datos
• Se cuenta con 2 enlaces a Internet[6] uno primario y otro secundario, cuando falla un enlace el otro debe entrar a soportar toda la carga de los Proxys, ya que se tienen actualmente dos proxys que reparten su carga de acceso a Internet entre los dos enlaces y aunque actualmente se tienen

[6] Enlace a Internet: medio físico como se provee un canal de datos para acceder a Internet.

mecanismos manuales para hacer esa distribución es importante que dichos mecanismos se realicen de manera automática. Es de aclarar que los servidores principales salen únicamente por el enlace primario.
• Falla en los dispositivos hardware tal como los enrutadores[7] de frontera o incluso el softwareicth[8] principal de Núcleo, que son equipos que permiten que haya conectividad, lo cual generaría un gran traumatismo de la red ya que no se tienen dispositivos de respaldo.
• Falla del servidor Web el cual soporta el Sitio y el portal institucional de la Universidad del Cauca que es la cara visible hacia Internet y por lo tanto al mundo, además que sobre este se soportan aplicaciones administrativas y educativas necesarias para las aplicaciones que se usan a diario.
• Fallo de los servidores de correo, lo cual genera un gran traumatismo para la Universidad del Cauca ya que por este medio se maneja información de suma importancia para el desarrollo de actividades educativas y de investigación que traen grandes beneficios para la comunidad educativa, por tal razón debido a su importancia dicho servicio no puede salir de funcionamiento.
• Fallo del servidor Proxy, el cual da acceso a Internet a casi la totalidad de usuarios activos que se tienen, una característica importante es que se tienen 2 servidores Proxy que acceden a Internet por dos enlaces diferentes, de tal manera que se distribuye el tráfico y se ofrece un servicio robusto.
• Fallo de los servidores complementarios que permiten que los servicios como el correo, WEB y Proxy puedan funcionar correctamente, lo cual implica que cuando están fuera de servicio se generen muchas perdidas de información y de continuidad en la prestación de los servicios.
• Fallos en la recuperación de la información, ya que al no tener un sistema de backup lo suficientemente grande para almacenar la información de Unicauca, se pueden presentar perdidas de información que no se pueden recuperar de manera rápida.
• No se tiene un plan de contingencia que permita reaccionar ante situaciones de daño o perdida de la información, lo que limita a los administradores y lo que seguramente se traducirá en tiempos mucho más largos para la puesta en funcionamiento del sistema.
• La contraseñas de los usuarios al no ser reguladas pueden ocasionar eventos inesperados como accesos no permitidos a los servicios, captura de información confidencial, por tal motivo se deben tratar a tiempo ya que ponen en peligro la información de los usuarios y la información del sistema en general.
• El Centro de Datos actualmente trabaja de una manera que se puede clasificar como eficiente, aunque muchos de los procedimientos que se realizan no se documentan de tal manera que se les pueda realizar un seguimiento formal que sirvan como base para que en futuras oportunidades se tenga un referente que permita actuar de una manera óptima.

2.4 Fallos y amenazas registradas

Esta información fue cedida por el administrador de dicha área a quien se le realizó una entrevista, obteniéndose de manera precisa referencias de alguna de las más importantes amenazas de las cuales han sido objeto los servidores, así como la manera en que se ha dado solución a dichas amenazas. No se cuenta con un documento claramente definido donde se consignen dichas amenazas y eventos no esperados, por lo tanto es de vital importancia generar el mecanismo que permita llevar a cabo este control para en una próxima situación poder darle una mejor solución a los problemas a los cuales se ha visto avocado. En la tabla 2.18 se consigna la información referente a estas situaciones.

[7] Enrutadores: equipos de red que funcionan en la capa 3 del modelo OSI, permiten la conectividad entre diferentes redes existentes.
[8] Softwareicth: equipos de red que funcionan en la capa 2 del modelo OSI, permiten interconectar redes dentro de una misma LAN.

Tabla 2. 18 Fallos y amenazas

Fallos	Descripción
Falta de infraestructura física.	Por la tecnología de red empleada en ese momento por sus características abría la puerta para que se presentarán muchos fallos de seguridad.
Empleo de herramientas y mecanismos no seguros para acceso a los servidores y equipos de red importantes.	Para el manejo de tráfico y servicios en el Centro de Datos, lo que hacia susceptible a la información de ser interceptada por personas no autorizadas.
Vulnerabilidades de los servicios.	Algunos como Apache, que al no estar debidamente actualizado con las mejoras de seguridad han permitido abrir puertas para posibles ataques.
Actualizaciones del sistema operativo.	Que permiten explorar e intentar aprovechar fallos de seguridad existentes.
Archivos de configuración de los servicios.	Debido a errores humanos en los cuales no se tenían en cuenta algunos parámetros o eran dejados sin la debida protección.
Intentos de acceso por fuerza bruta.	Constantemente se detectan intentos de acceso los servidores por ataque de fuerza bruta. Hasta el momento no se tiene precedente de intrusiones.
Acceso por shell brindado a los usuarios.	Uno los grandes inconvenientes que se presentan y en especial a los servidores es el acceso que se le brinda a los usuario por SSH, ya que un usuario al tener acceso a shell de un servidor tiene muchas mas posibilidades de ocasionar un fallo o de tener acceso no autorizado.
Vulnerabilidades de Aplicaciones empleadas por usuarios.	Se puede enumerar Moodle[9] la cual presenta grandes fallos de seguridad.
Permisos que se le brinda a los usuarios de aplicaciones y sitios Web.	Estos permisos facilitan la introducción de errores humanos y elementos que pueden generar posibles brechas de seguridad.

Estadísticas de puertos abiertos en los servidores

Tabla 2. 19 Datos obtenidos desde la red interna

Puerto abierto Red interna	Número de Servidores	Puerto abierto red externa	Número de Servidores
21	5	20	5
22	9	21	5
23	1	22	5
25	4	25	2
42	1	53	2
53	3	80	5
80	8	109	2
88	1	110	2
110	2	143	2
111	6	220	2
113	6	443	2
135	2	587	2
139	2	993	2
443	3	995	2
445	2	1718	1
8080	2	1719	1
		8000	1
		8009	1

[9] Moodle: aplicación que permite crear sitios Web académicos de manera dinámica.

		8080	1
		8443	1

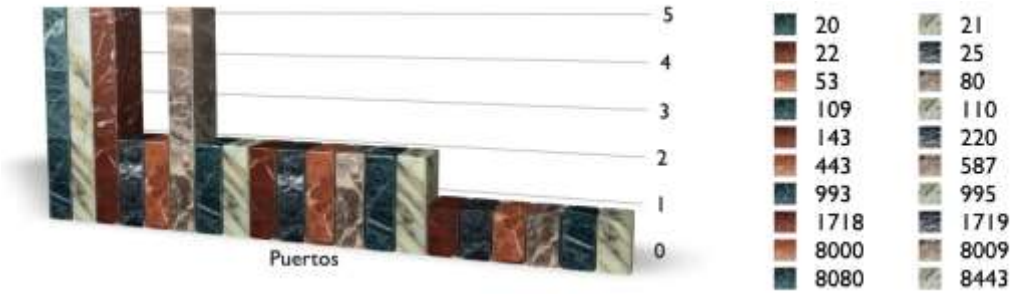


Figura 2. 6 Datos obtenidos desde una red externa

De las tablas 2.19 y 2.20 se puede observar que en general los servidores se encuentran con una gran cantidad de puertos abiertos, lo cual es lógico por las aplicaciones que se tienen en funcionamiento, pero algunos de esos puertos son no conocidos o corresponden a aplicaciones desconocidas o que por sus características y naturaleza presentan una brecha de seguridad y abren las puertas para explotar vulnerabilidades, por lo tanto dichos puertos deben ser considerados y se deben mirar la posibilidad de restringir su acceso, así como implementar mecanismos de seguridad que permitan mantener un control de los mismos y si es preciso se puede plantear la posibilidad de cerrarlos o bloquearlos.

La figura 2.7, obtenida con la herramienta *keynote,* muestra las estadísticas de puertos abiertos con mayor frecuencia, lo que también indica cuales son los servicios más importantes que se prestan actualmente. Se puede observar que los principales servicios son el Web que corresponde al puerto 80, el FTP, el DNS, el correo electrónico y SSH. Servicios esenciales que son prestados por el Centro de Datos.

Figura 2. 7 Porcentaje de puertos abiertos

Tabla 2. 20 Fallos encontrados en el análisis

Posibles fallas y elementos que afectan el funcionamiento
Los servicios se ven comprometidos ya que al solicitar información, en los puertos correspondientes, estos muestran la versión actual que esta instalada.
Se presentan algunos problemas debido a los directorios con permisos muy amplios o con accesos a cualquier tipo de usuario, esto se presenta para algunos usuarios.
El servicio Web soporta métodos cómo trace y track, los cuales son métodos para analizar las condiciones de servidor Web, estos métodos hacen vulnerable el servicio a ataques de crosssite-site-scripting[10], el cual puede ser usado en conjunto con las vulnerabilidades del navegados WEB. Para explotar un fallo.
Posiblemente los servidores Web, son susceptibles de ataques con scripts crosssite, esta vulnerabilidad es causada cuando se le retorna al usuario el resultado de un archivo que no existe. Es decir pueden usar código java script para generar inconvenientes, ejemplo de una url: HTTP://10.200.1.137:8009/<SCRIPT>foo</SCRIPT> Solución: visitar periódicamente las páginas respecto a la versión del servicio instalada para ver posibles fallos o errores encontrados en los servicios.
Se tienen inconvenientes en los servidores tanto Apache como Tomcat, ya que los archivos que se mantienen como ejemplo de configuración permiten observar información relevante a la versión exacta que se tiene instalada.
El puerto 443 de SSL devuelve información importante con respecto a los certificados digitales de seguridad.

2.5 Definición de activos

Los activos son aquellos elementos que son importantes para una organización, para este caso son los elementos importantes para el Centro de Datos, tales como equipos, software, personal. Instalaciones, etc. Entre estos se pueden determinar los principales elementos a considerar como lo son los servicios, los datos, el software, los cuales son percibidos por los usuarios de una manera más amplia y detallada, a continuación se enumeran los activos mas importantes y algunos de manera estadistica, para una información mas completa de los elementos que hacen parte del Centro de Datos, se puede remitir a la información que se encuentra referenciada en el documento completo de análisis de riesgos el cual hace parte y es propiedad del área de servicios y servidores de Internet, el cual es clasificado como un documento que contiene información confidencial. En la tabla 2.21 se presentan los servicios más importantes, discriminados por el nombre del equipo que lo contiene y los servicios que actualmente se encuentran configurados. Así como las aplicaciones software que corren sobre los equipos mencionados para soportar los servicios que se ofrecen:

[10] Crosssite-site-scripting: es un ataque basado en la explotación de vulnerabilidades del sistema de validación de html incrustado.

Tabla 2. 21 Servicios soportados en el Centro de Datos

Nombre del Equipo	Servicios soportados	Aplicaciones informaticas	Sistema Operativo
Acuario	FTP, HTTP, Hosting, bases de datos, SSH, tomcat	VsFTP, Apache, mysql, openSSH, jakarta-tomcat	Debian Linux
Afrodita	FTP, HTTP, IMAP, POP, smtp, SSH	VsFTP, Apache, Cyrus, Uw, postfix, openSSH	Debian Linux
Atenea	FTP, HTTP, IMAP, POP, SMTP, SSH	VsFTPd, Apache, Cyrus, Uw, Postfix, openSSH	Debian Linux
Cronos	Servicio Dns de windows	Dns server	Windows 2003 Server
DNS1	Dns, SSH	Bind9, openSSH	Debian Linux
Dns 2	Dns, SSH	Bind9, openSSH	Debian Linux
Gestion servidores	Gestion de ancho de banda Gestion de servidores y servicios Gestion de enlaces de internet. Gestion de logs awstats Gestion de logs acuario Radius autenticación de acceso remoto Streaming de la emisora. HTTP, analisis de logs proxy	Netexplorer Nagios-text, Netflow Mrtg Awstats Webalizer Freeradius Icecast2 Apache, Sarg	Debian Linux
Hades	Dns windows, escritorio remoto, servicio web	Tsclient, IIS	Windows 2000 Server
Hiperion	Proxy, SSH	Squid, openSSH	Debian Linux
Temis	Proxy, SSH	Squid , openSSH	Debian Linux
Hera	Autenticaciòn de usuarios, enrutamiento de correos, SSH	Openldap, openSSH	Debian Linux
Juno	Autenticaciòn de usuarios, enrutamiento de correos SSH	Openldap, openSSH	Debian Linux
Netexplorer	Administración de ancho de banda, java	Netexplorer, j2sdk	Windows 2003 Server
Odin	Servicio de FTP	VsFTPd, Scponly	Debian Linux
Perseo	Asignación dinámica de direcciones	DHCPD	Debian Linux
Ares	Firewall	Cisco pix firewall version 6.3(4)	Cisco pix device manager version 3.0(2)
Arges	Firewall	Iptables	Debian Linux
Fortigate, fortianalyzer	Detección de spam	Fortigate-100 A	FortiOS

2.5.1 Los datos

La información que se maneja en gran porcentaje es de contenido académico, representada en la producción intelectual de docentes y estudiantes, así mismo información académica de grupos y procesos de investigación y en general de la comunidad educativa. Adicional a esto se manejan datos de carácter administrativo para la administración de los procesos normales de la Universidad del Cauca, los cuales implican un alto nivel de seguridad e integridad por las características de la información

que se maneja**.**

Tabla 2. 22 Datos

Datos	Tipo de datos	Descripción
Datos de administración.	Datos vitales.	Agrupan el conjunto de datos que son de vital importancia para los procesos administrativos internos que realiza.
Datos de carácter Institucional.	Datos vitales.	Comprende la información referente a dependencias, facultades, grupos de investigación, que hacen parte.
Datos ámbito educativo.	Datos vitales.	Información referente a necesidades en cuanto a aplicaciones programas software y la producción intelectual del personal que hace parte de la Universidad.
Datos de gestión interna.	Datos vitales.	Manejados por cada dependencia y facultad, en cuanto a registros, notas, calificaciones e información importante para el desempeño de las labores educativas.
Datos de carácter personal.	Servicios Web personal de cada usuario E-mail.	Datos y aplicaciones personales de cada usuario, la información relevante, los correos electrónicos y la información que manipulan desde su propia Web.
Multimedia.	Emisora.	Difusión hacia Internet de la radio universidad del Cauca.
Código fuente.	Datos vitales.	Aplicaciones desarrolladas por el equipo de desarrollo de la red de datos, para realizar la gestión de servicios y tareas administrativas.
Datos de configuración.	Servicios esenciales del Centro de Datos.	Configuración de los servicios soportados para la prestación de los servicios importantes.
Datos de registro de actividad.	Logs de los servicios implementados en el Centro de Datos.	Logs de la actividad y funcionamiento diario de los servicios que actualmente se están soportando.
Datos de prueba.	Servicios que se encuentran en fase experimental.	Actualmente realizada por el área de servicios y servidores de Internet.

2.5.2 Aplicaciones software

Se cuenta con un equipo de desarrollo que ha venido automatizando tareas que se realizaban de manera manual, las aplicaciones se han desarrollado sobre diferentes plataformas de programación como Php, Java, Jmf y Xml y se han alojado sobre los servidores del Centro de Datos. Estas aplicaciones se desarrollan para la gestión de contenido, manejo de usuarios, automatización de procesos y requerimientos puntuales de cada dependencia, en la tabla 2.23 se encuentran las aplicaciones que se emplean para la prestación de los servicios.

Tabla 2. 23 Aplicaciones software

Nombre Aplicación	Tipo Aplicación	Descripción
Aplicaciones desarrolladas para automatizar procesos de	Desarrollo propio.	Administración de tareas y procesos de dependencias.

gestión y administración de recursos del área administrativa.		
Web mail.	Desarrollo propio.	Aplicación para hacer uso del correo electrónico.
Pericles.	Desarrollo propio.	Aplicación para gestión de la sala de navegación de la red de datos.
Administración red.	Desarrollo propio.	Para mantener actualizados los datos de los integrantes de la red de datos.
Apache.	Servicio de presentación (estándar).	Servidor presentación, donde se encuentran alojados la pagina principal de la Universidad del Cauca, así como los demás sitios de las dependencias que lo conforman.
Squid.	Proxy (estándar).	Servidor Proxy sustituto que permite dar acceso a Internet a más de dos mil terminales que se encuentran habilitados para hacerlo.
VsFTPd.	FTP estándar.	Servidor para la administración de contenido.
Bind9 (DNS).	Estándar.	Servidor para resolución de nombres.
Dhcpd (DHCP).	Estándar.	Servicio para asignar direcciones IP automáticamente.
Postfix (Email-server).	Estándar.	Servicio de correo electrónico para los usuarios perteneciente a la Universidad del Cauca.
Clamav (antivirus).	Antivirus Estándar.	Antivirus para los servidores de correo.
Spamassasin antivirus.	Antivirus Estándar.	Servicios para detectar Spam, del servicio de correo electrónico.
Yakarta-tomcat.	Servidor de presentación	Servicio para dar soporte a las aplicaciones desarrolladas sobre java.
J2sdk.	Servicio java estándar.	Para dar soporte a las aplicaciones que corren sobre java.
Openldap (LDAP).	Estándar.	Servicio de directorio para administración de usuarios y de enrutamiento de los correos.
Nagios-text.	Estándar.	Servicio para gestión de los equipos de red y servidores del Centro de Datos.
OpenSSH.	Estándar.	Servicio para conexión remota desde clientes externos a los servidores.
IPtables.	Estándar.	Para configuración de reglas y políticas de acceso y seguridad del Firewall.
Icecast2.	Estándar.	Para multidifusión IP de la emisora de la universidad del Cauca.
Freeradius, (Radius).	Estándar.	Servidor de autenticación de usuarios remotos que hacen uso del acceso a Internet desde su casa.
Netflow.	Estándar.	Para gestión del ancho de banda y el tráfico interno.
Awstats.	Estándar.	Gestión de Logs de los sitios virtuales, para generación de estadísticas graficas.
Webalizer.	Estándar.	Gestión de Logs para generación de estadísticas graficas del sitio Web.
Sarg.	Estándar.	Análisis de Logs para generación de estadísticas graficas del consumo y actividad de los proxys.
Mrtg.	Estándar.	Gestión del enlace externo para el acceso a Internet.
Debian sarge 3.1	Sistema Operativo.	Sistema operativo para algunos servidores que soportan los servicios.
Windows 2000 server.	Sistema Operativo.	Sistema operativo para algunos servidores que soportan los servicios.
Windows 2003 server.	Sistema Operativo.	Sistema operativo para algunos servidores que soportan los servicios.
Netexplorer.	Software propio del gestor de ancho de banda..	Empleado para administración del ancho de banda y regulación de las aplicaciones y el tráfico hacia Internet.
Backups.	Servidor de backups.	Para realizar copias de seguridad de los equipos servidores del Centro de Datos.

2.5.3 Hardware

Se cuenta con su propia infraestructura física, de red y con sus propios servidores y equipos para soportar los servicios esenciales que ofrece, dichos servidores son equipos diseñados para soportar estos servicios, además tienen muy buenas características que garantizan un buen funcionamiento y desempeño. En la tabla 2.24 se presenta una discriminación de los servicios que se soportan, de acuerdo a su nombre y las características del equipo sobre el cual está alojado.

Tabla 2. 24 Hardware

Servicio soportado por el Servidor	Descripción
WEB.	Servidor en rack, DELL PowerEdge 1950.
FTP.	Dell PowerEdge 800.
DNS externo principal.	Sun ultra 10.
DNS externo secundario.	Sun ultra 1.
DNS interno principal.	Dell PowerEdge 1600 SC.
DNS interno secundario.	Dell Optiplex Gx 240.
Correo para docentes y administrativos.	Servidor en rack, DELL PowerEdge 2850.
Correos para estudiantes.	Servidor en rack, DELL PowerEdge 2850.
Proxy.	Dell PowerEdge 4200.
Proxy.	Dell PowerEdge 4200.
Enrutamiento de correos y directorio de usuarios.	Servidor en rack, DELL PowerEdge 1425.
Enrutamiento de correos y directorio de usuarios.	Servidor en rack, DELL PowerEdge 1850.
DHCP.	Premio Pentium II.
Firewall.	Dell Optiplex Gx 240.
Gestión de red.	Dell PowerEdge 2400.
Netexplorer.	Dell Optiplex Gx 280.
Administrador del ancho de banda ALLOT.	Equipo de red en rack, Netenforcer Ac-404.
Servidor de acceso remoto.	Equipo de red en rack, Remote Access Server 2960
Detector de Spam.	Fortigate 100 A.
Analizador y generador de reportes de Spam.	Fortianalizer 100 A.
Firewall.	Firewall Cisco pix 515e.
Switch de núcleo.	Switch Cisco Catalyst 4507.

2.5.4 Redes de comunicaciones

Se tiene una infraestructura de red propia, donde se cuenta con equipos de red de altas capacidades ya que su núcleo interno tiene equipos con capacidades nominales de 1000 Megas.

Los equipos servidores del Centro de Datos se encuentran conectados al Switch de

núcleo, dicho equipo tiene la capacidad de soportar VLANS, lo que permite una separación y segmentación del tráfico que está en la red, además que ayuda a disminuir las brechas de seguridad.

Tabla 2. 25 Redes de comunicaciones

Tipo de red	Descripción
Red local [LAN].	Red de área local con equipos con capacidades que permiten la segmentación por Vlans, actualmente solo se cuenta con la separación de la red de lo servidores, los demás sitios de la Universidad se encuentran en procesos de implementación.
Red Metropolitana [MAN].	Red de Accesos a Internet, la cual no es administrada por el Centro de Datos, además de que se tiene dos enlaces. Uno principal de 8 Mbytes contratado con Emtel y un secundario de 7 Mbytes contratado con ETB

2.5.5 Soportes de información

El Centro de Datos tiene implementado un sistema para realizar copias de respaldo de la información, que se realizan sobre los discos duros de los equipos, anteriormente se tenía un procedimiento por *tape backups* que consistía en una cinta en la cual se comprimía la información referente a los correos de los estudiantes, los docentes y de las bases de datos, actualmente no se realiza *backups* en cintas magnéticas o medios extraíbles, se tiene un intercambiador de cintas con capacidad para 8 cintas cada una de 400 gigas, que se encuentra en proceso de implementación.

Tabla 2. 26 Soportes de información

Dispositivo	Descripción
Tape backups	Intercambiador de cintas marca Dell con capacidad para el manejo de 8 cintas cada una con capacidad de almacenar hasta 400 Gigas, aun no se encuentra en operación.
Servidor discos (*disk*)	Donde actualmente se realizan los *backups* de información de correos de estudiantes, de docentes, de administrativos, con su respectivo directorio personal, de igual manera se realiza un *backup* de las bases de datos y de los sitios que se encuentran alojados en el servidor Web.
Servidor para gestión de servidores (*disk*)	Realiza los *backups* de la información de sucesos (Logs) de los servicios Web, página principal y los sitios virtuales, también del acceso a Internet por medio de Proxy.

2.5.6 Equipamiento auxiliar

Cuenta con un sistema de respaldo para fallos de energía que consta de un conjunto de UPS, que tienen en condiciones optimas y para la cantidad de equipos que se tienen, una autonomía de 5 horas, pero en este momento unas están fallando y el tiempo máximo de durabilidad es de 15 minutos, después de los cuales sale de funcionamiento.

Tabla 2. 27 Equipamiento auxiliar

Dispositivo	Características
UPS.	Los sistemas de alimentación interrumpida de los cuales consta el Centro de Datos, son actualmente dos circuitos los cuales tienen una autonomía de funcionamiento de 5 horas pero por problemas técnicos actualmente no son capaces de soportar mas de 15 minutos la carga del sistema.
AC equipos de climatización.	Se cuenta con un sistema de refrigeración que mantiene el Centro de Datos en un ambiente óptimo que impide el deterioro de los equipos y soportes de información, este sistema actualmente se encuentra en funcionamiento.
Mobiliario.	Cuenta con dos rack para soporte de equipos de red y un armario para soportes de servidores en rack, así mismo cuenta con dos mesas para soportar los otros servidores que no se pueden acomodar en el armario para servidores.

2.5.7 Instalaciones

Actualmente el Centro de Datos de la Universidad del Cauca tiene las instalaciones en el Instituto de Postgrados de Ingeniería Electrónica de la Universidad del Cauca sector Tulcán, este es el bastión principal de la infraestructura de red, este a su vez cuenta con sedes ubicadas en el edificio de sistemas donde trabaja el personal.

Tabla 2. 28 Instalaciones

Lugar	Descripción
IPET.	Donde se alojan los servidores y los equipos de red tales como Enrutadores, Switchs, equipos de red y servidores que garantizan el acceso a Internet.
Sistemas.	Ubicado en el edificio de ciencias naturales y exactas, donde se encuentran las instalaciones del personal administrativo y técnico que hacen parte del Centro de Datos de la Universidad del Cauca

2.5.8 Personal

Las personas que realizan la administración de los servidores y los equipos de red del Centro de Datos se encuentran distribuidas en un jefe de área y cuatro monitores que realizan la administración de los servicios soportados, así mismo los servicios prestados por el Centro de Datos presenta diferentes roles, como estudiantes, docentes, egresados y el personal administrativo, mas información sobre los usuarios en la tabla 2.30.

Tabla 2. 29 Personal

Personal	Categoría	Descripción
Proveedores Usuario.	Externos.	Son las terceras partes con quienes se contrata los accesos a Internet por medio de los dos enlaces que se tienen con ETB y Emtel.
Egresados Usuario.	Externos.	Son usuarios externos que hacen uso de los servicios de la Universidad como el correo electrónico y el alojamiento de un sitio Web en sus propios directorios personales.

Área de servidores Root.	Administrador.	Conformado por un ingeniero jefe de área y cuatro estudiantes como monitores, de los cuales tres cubren un turno completo durante la semana, los tres estudiantes tienen el mismo rol de administradores de los equipos y cumplen las mismas funciones.
Área de desarrollo Usuario privilegios ejecución.	Interno, operador.	Este equipo de trabajo esta conformado por cuatro monitores y un ingeniero jefe de área, quienes desarrollan aplicaciones para automatizar procesos y solo tienen dominio sobre su propio sistema y sobre los directorios asignados.
Docentes Usuario	Interno	Hacen uso del servicio de correo electrónico, además del servicio de *hosting* para alojar en sus directorios personales sus propias páginas Web, su directorio se aloja sobre atenea. Su perfil de usuario tiene privilegios adicionales que no tienen los estudiantes.
Estudiantes Usuario	Interno	Hacen uso del servicio de correo electrónico, además del servicio de *hosting* para alojar en sus directorios personales sus propias páginas Web, su directorio se aloja sobre afrodita.

2.5.9 Dependencia entre activos

Para el Centro de Datos de la Universidad del Cauca, y para la realización del análisis entre las dependencias entre activos se empleó un modelo de capas como el mostrado en la tabla 2.31.

Tabla 2. 30 Dependencia entre activos

Nombre	Contiene
Capa 1.	Activos de orden inferior los cuales se requieren para garantizar el correcto funcionamiento de los equipos, suministros de energía, climatización y comunicaciones.
Capa 2.	El sistema información que comprende activos como hardware, para éste caso los servidores y equipos de red que permiten interconexión y soporte de las aplicaciones que hacen posible que el Centro de Datos preste a la comunidad universitaria los servicios esenciales, sin olvidar que es importante el soporte de información como discos, cintas y procedimientos para realizar copias de seguridad.
Capa 3.	Contiene los activos de mayor orden como lo son la información, los datos y las estructuras lógicas que se mantienen para guardar información, se puede mencionar la información de carácter educativo e información de carácter administrativo para los procesos internos.
Capa 4.	Las funciones o servicios que presta la Universidad del Cauca los cuales justifican la razón de ser del Centro de Datos, dentro de estos se puede mencionar los servicios esenciales para acceso Internet y los servicios complementarios que permiten a los usuarios hacer uso de recursos como el correo electrónico, el servidor Web y las aplicaciones desarrolladas a medida para cada caso especial.
Capa 5.	Información como ponencias, producciones intelectuales, información personal y relevante de cada usuario, además cursos que permiten que la Universidad cuente con un buen nombre el cual es importante mantener, por lo tanto la cara visible de la Universidad, su portal Web, se debe mantener en las mejores condiciones de tal forma que sea siempre visible y que este catalogado de la mejor manera, garantizando calidad y confianza.

La realización del análisis de dependencia entre activos se realiza tomando los grupos de clasificación que encierran los diferentes tipos de activos, los resultados de este proceso se pueden ver plasmados en la tabla 2.31, en el cuadro se puede observar el nivel de

dependencia que tienen los activos, por un lado se observa que los servicios son uno de los elementos más importantes con los que se cuenta y su nivel de dependencia con otros activos es alto, ya que para poder prestar su funcionalidad requiere del hardware, de los datos, de las redes de comunicaciones incluso de todos activos que hacen parte de dicho centro de datos, aunque se puede expresar que tiene mayor dependencia de las aplicaciones informáticas y el hardware que permiten que dichos servicios funcionen adecuadamente, por otro lado están los datos, los cuales son muy importantes pero requieren de los servicios, también tienen una gran dependencia de las aplicaciones informáticas que se soportan. En el diagrama se nota el grado de dependencia y es de notar que el personal es un factor clave para el funcionamiento ya que es un activo fundamental, que tiene la potestad de garantizar el buen funcionamiento, pero en determinadas ocasiones, ya que muchos de los servicios se prestan de manera automática y la dependencia entre activos va disminuyendo conforme las situaciones tienen un funcionamiento normal.

Tabla 2. 31 Dependencia entre activos

	Servicios	Datos	A_informaticas	Hadware	R_comunicaciones	S_informacion	E_auxiliar	Instalaciones	Personal
Servicios		✓	✓	✓	✓	✓	✓	✓	✓
Datos	✓		✓	✓	✓	✓			✓
A_informaticas				✓	✓				
Hadware							✓	✓	✓
R_comunicaciones							✓	✓	✓
S_informacion				✓					✓
E_auxiliar								✓	✓
Instalaciones									
Personal									✓

A_informaticas = Aplicaciones informáticas:

R_comunicaciones = Redes de comunicaciones:

S_informacion = Soportes de Información:

E_auxiliar = Equipamiento auxiliar:

2.5.10 Valoración de los activos

Indiscutiblemente para el Centro de Datos la información que maneja y los servicios que

prestan son el pilar fundamental y su razón de ser, es muy importante la información de carácter institucional, académica, administrativa y de investigación, pero esta información sin los servicios es poco útil. La prestación eficaz de estos servicios y la administración de la información no es posible sin la utilización de equipos que puedan suplir las características de funcionamiento, así mismo sin la utilización de un adecuado lugar físico que cumpla con los requerimientos necesarios, sin olvidar que debe contar con el personal idóneo que sea capaz de dar una adecuado manejo a la información alojada y los servicios prestados, por tal motivo los datos y los servicios son el principal activo del Centro de Datos de la Universidad del Cauca.

Los servidores y equipos de aplicaciones: tienen un alto valor, ya que cualquier fallo de estos puede generar grandes pérdidas y grandes consecuencias, dentro de estos se encontró unos con un nivel de valoración alto.

Los equipos de red: Son equipos vitales ya que el correcto funcionamiento de estos permite la interconexión de los servidores con la red interna y con Internet, en la tabla 2.33 se enumeran algunos de mayor importancia:

Tabla 2. 32 Descripción equipos importantes

Tipo de equipo	Descripción
Servidor WEB	Cuenta con una alta prioridad ya que es la cara visible desde Universidad del Cauca hacia Internet.
Servidor de correo	Su nivel de prioridad es alto, debido a las características de la información que se maneja por este medio.
Servidor Proxy	Dicho servidores son muy importante para la navegación, su salida de funcionamiento genera un grave traumatismo, pero este servicio se encuentran en redundancia por lo tanto su prioridad no es tan alta.
Servidor DNS	Aunque actualmente se cuenta con dos servidores de este tipo, la falla de uno de los o de los dos servidores ocasionaría grandes traumatismos ya que sin este servidor los correos muy posiblemente se perderían, el portal Web no sería visible y la navegación tampoco podría realizar su función, por tal motivo es un servidor muy importante.
El servidor de autentificación y enrutamiento:	Dicho servidor es muy importante ya que son los que permiten que los servicios de correo puedan funcionar de manera correcta y óptima.
Switch de núcleo 4507	Es uno de los más importantes ya que tiene la responsabilidad de comunicar todas las sedes con las que se cuenta en la red.
Switch 3750	Son los equipos que se han ubicado en las sedes principales de la Universidad y permiten la interconexión de las diferentes sedes que se tiene.
HUB	Son los equipos de red de la Universidad y son los encargados de recibir a la gran mayoría de usuarios con los que cuenta la red de datos.
Enrutadores	Son los equipos de red encargados de dar acceso a los servidores de Internet, la función de dichos equipos es vital importancia debido a que la falla de ellos

	incomunicaría la red de la Universidad del resto de redes de Internet.
Firewall	Son los equipos que permiten dar protección a la red interna, dichos equipos son de vital importancia, ya que su mal funcionamiento puede generar inconvenientes que impedirían el normal funcionamiento de las aplicaciones y los servicios con los que cuenta..
La infraestructura de red.	Aunque no le corresponde directamente centro de datos es importante debido a que cualquier daño en la infraestructura puede causar grandes inconvenientes e incluso puede sacar de funcionamiento el centro datos.
El equipamiento auxiliar	Cuenta son equipos tales como suministros de energía, aire acondicionado, baterías y UPS, los cuales son elementos indispensables para el correcto funcionamiento del centro datos cualquier fallo en algunos de estos elementos ocasionaría que el centro de datos se vea abocado en una situación de crisis ya que saldría de funcionamiento por tal motivo su valoración es alta.

La figura 2.8 creada con la herramienta *Paint*, muestra la escala de valoración, para esta se determino una escala de 1 a 10, la cual tiene valores desde despreciable hasta muy importante, para este caso se va a realizar con subgrupos.

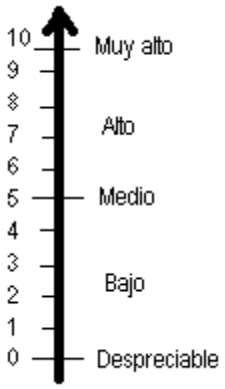


Figura 2. 8 Escala de valoración

Tabla 2. 33 Descripción de los valores y criterios

Valor		Descripción
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización.
4-6	Medio	Daño importante a la organización.
1-3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Con la escala anterior y con los subgrupos formados se realizó la valoración de los activos y estos se encuentran consignados en la tabla 2.34:

Tabla 2. 34 Valoración de activos

Activo		**Valoración**
Servicios	Web	10
	Proxy	8

	Correo	9
	DHCP	5
	DNS	9
	FTP	7
	LDAP	9
	RAS	7
Datos	Configuración	10
	Administración	10
	Educativos	9
	Personales	8
Software	Aplicaciones Unicauca	9
	Aplicaciones servicios	9
Hardware	Servidores	9
	Equipos de red	8
Recursos comunicaciones		8
Soportes Información		5
Equipamiento auxiliar		6
Instalaciones		9
Personal		10

La anterior es una valoración global con la herramienta de análisis de riesgos se puede discriminar y realizar una valoración mas exacta de dichos activos.

2.5.11 Dimensiones de valoración de los activos

Tabla 2. 35 Dimensiones de valoración

Autenticidad
• Los servicios esenciales como lo son el correo electrónico, el servidor Web, y el acceso aplicaciones importantes emplea mecanismos que solicitan el uso de contraseñas, sin estas no se puede acceder a los servicios donde se tiene acceso. • Los usuarios pueden acceder como usuarios con privilegios restringidos a los servidores donde se encuentran los servicios soportados, el usuario root tiene la capacidad de acceder a toda la información. • No se puede determinar que usuarios hacen uso de la infraestructura con la que se cuenta para navegación, ya que no se tiene una base de datos completa donde se regristen los accesos.
Confidencialidad
• Los servidores de correo electrónico, no se puede garantizar que solo el destinatario va a recibir dicha información, ya que el correo no se envia por medios cifrados. • La información solo puede ser accedida por el propietario, • Los servidores de aplicaciones manejan información de los usuarios, por lo cual no se puede garantizar que la información solo sea accedida por el propietario ya que estos tienen la potestad para colocar privilegios y en ocasiones los dejan abiertos para cualquier usuario. • La confidencialidad de los archivos de configuración y de los servicios y servidores del Centro de Datos se garantiza en gran medida ya que los archivos cuentan con los mecanismos y controles para este objetivo.
Integridad
• La información almacenada en los servidores cuenta con copias de respaldo, pero esto mecanismos no son suficientes para garantizar la integridad dicha información, ya que dichas copias de respaldo se realizan en determinados momentos. • Los datos de configuración de los servidores y los equipos de red deben garantizar su total integridad ya que cualquier manipulación genera grandes traumatismos en los servicios aplicaciones, pero esto se realiza de manera manual lo que puede introducir cambios o daños.

Disponibilidad
• Las personas encargadas de administración y gestión de los equipos conocen de facto que equipos y que servidores son importantes y que por lo tanto se les debe dar la mayor prioridad pero no se tiene claramente definido. • No se cuenta con los suficientes mecanismos que permitan que los servicios estén en funcionamiento durante las 24 del día los siete días de la semana. • Los suministros auxiliares como fuentes de energía baterías alternas y equipos de refrigeración no cuentan con sistemas de respaldo y algunas como las UPS se encuentran en un estado de funcionamiento limitado.
Trazabilidad del servicio
• Se realiza por medios manuales, es decir se leen y analizan archivos de logs del sistema, lo que es un mecanismo que cuenta con muchas vulnerabilidades ya que lo hace susceptible a fallos o alteraciones que pueden cambiar esta información. • No se tiene actualmente un sistema para determinar quién o que accedió a los servicios, servidores o elementos de la infraestructura de red para esta manera determinar donde se pueden estar presentando posibles fallos de seguridad. Al implementar una aplicación para los servidores y las aplicaciones se puede llevar un control detallado de que equipos están siendo accedidos indebidamente y qué consecuencias están generando dichos accesos.
Trazabilidad de los datos
• No se tiene ningún mecanismo que permita realizar estos procedimientos en el Centro de Datos

2.6 Valoración de amenazas

Una valoración amenazas es un proceso difícil, se trata de tener en cuenta todas las amenazas que pueden afectar un sistema el cual no tiene implementado ningún tipo de medidas de protección, lo cual lo convierte en una tarea muy difícil, ya que se pueden presentar múltiples situaciones las cuales son muy difíciles de prever debido a situaciones que son anormales. Debido a esto el análisis de amenazas se ha realizado teniendo en cuenta los estudios y los resultados de otros procesos los cuales han permitido generar mecanismos y valoraciones estándar que a pesar de tratar de manera amplia los sistemas permiten obtener una valoración bastante aproximada y además la cual se puede acoplar a las características de cada organización.

Para la realización de la tabla 2.37 donde se consignan las amenazas, los activos y las dimensiones de valoración se emplean las convenciones de la tabla 2.36, las cuales permiten que el diseño de las tablas se haga más pequeños:

Tabla 2. 36 Convenciones

Letra	Descripción
D	Disponibilidad
A	Autenticidad
I	Integridad
C	Confidencialidad
A_S	autenticidad los usuarios del servicio

A_D	autenticidad del origen de datos
T_D	Trazabilidad de los datos
T_S	Trazabilidad de los servicios
N	Desastres naturales: fuego, daños por agua.
I	De origen industrial.
E	Errores y fallos no intencionados.
A	Ataques intencionados.
(S)	Servicios
(D)	Datos
(SW)	Software
(HW)	Equipos informáticos
(COM)	Redes de comunicaciones
(SI)	Soportes Información
(AUX)	Equipamiento Auxiliar
(I)	Instalaciones
(P)	Personal

Tabla 2. 37 Amenazas estándar que pueden afectar al Centro de Datos

Tipo de amenaza		**Activos**	**Dimensiones de Valoración**
Desastres naturales	Fuego	HW,COM,SI.AUX,I	D, T_D , T_S
	Daños por agua	HW,COM,SI.AUX,I	
Origen industrial	Fuego	HW,COM,SI.AUX,I	D, T_D, T_S
	Daños por agua	HW,COM,SI.AUX,I	
	Desastres industriales	HW,COM,SI.AUX,I	
	Contaminación electromagnética	AUX,I,HW,COM	
	Averías de tipo físico y lógico	SW,HW,AUX,I,SI	
	Corte suministro eléctrico	HW,AUX,I	
	Condiciones inadecuadas de humedad	I, HW,AUX,I	D, T_S, T_D
	Fallos en los servicios de comunicaciones	COM	D
	Interrupción de los suministros y servicios esenciales	AUX	D
	Degradación de soportes de almacenamiento de información	SI, D	I, A
Errores y fallos no intencionados	Errores de administrador	D, S, HW,COM	D, I, C, T_S, T_D
	Error de usuarios	S, D, COM	D, I
	Error de registros monitorización	SW,S,D	T_D, T_S
	Error de configuración	SW,S,D, HW	T_D, T_S
	Difusión de software dañino	SW, D	T_D, T_S
	Errores de re-encaminamiento	D, COM	D, I, A
	Errores de secuencia	D, COM	D, I, A
	Escapes de información	D, SW	I, A
	Alteración de la información	D	I
	Introducción de información incorrecta	D,SW,S	I, A
	Degradación de la información	D, S	I
	Destrucción de la información	D	I
	Divulgación de la información	D	I
	Vulnerabilidad de programas	SW, D	I, A, D, T_S
	Errores de mantenimiento y actualización de programas	SW	I, D, T_S
	Errores de mantenimiento y actualización de programas	HW	I, D
	Caída del sistema por agotamiento de recursos	SW, HW, D	D, I, A, T_S, T_D

	Indisponibilidad del personal	P	D, I, A, T_S, T_D
Ataques intencionados	Manipulación de la configuración	SW, HW, D, S	A, I
	Suplantación de la identidad	D	A
	Abuso de privilegios de acceso	SW, HW, S	I, D, A
	Uso no previsto	HW, S, D	I, D
	Difusión de software dañino	SW	I
	Alteración de secuencia	SW, D, COM	D,I,A
	Re-encaminamiento de mensajes	COM, D	D,I,A
	Acceso no autorizado	COM, HW, SW, S	D, I, A
	Análisis de tráfico	COM	
	Repudio	D, S, SW, HW	I, A, D
	Interceptación de información	D, S, SW, COM	I, A, D
	Introducción de falsa información	D, S	I, A, T_D
	Corrupción de la información	D	I, A
	Divulgación de la información	D	I
	Manipulación de programas	SW	I, A
	Denegación de servicios	D, S, SW, HW, COM	D
	Robo	D	I, A
	Ataque destructivo.	D, SW, HW	D, I, A, T_S, T_D
	Indisponibilidad del personal	P	D, I, A
	Ingeniería social	P, D	D, I, A

Es importante tener en cuenta que los errores y ataques que se presentan pueden ser por:

- Amenazas que siempre pueden ser errores nunca ataques deliberados.
- Amenazas que nunca son errores siempre son ataques deliberados.
- Amenazas que pueden producirse por error como deliberadamente.
- Al respecto es conveniente determinar que tipo de amenazas se pueden considerar como error y cuales se pueden considerar como ataque o una vulnerabilidad de seguridad.

- **Tabla 2. 38 Relación de errores y ataques**

Número	Error	Ataque
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización *(log)*	
4	Errores de configuración Manipulación de la configuración	
5		Suplantación de la identidad del usuario
6		Abuso de privilegios de acceso
7	Deficiencias en la organización Uso no previsto	
8	Difusión de software dañino	Difusión de software dañino
9	Errores de [re-]encaminamiento	[Re-]encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11	Acceso no autorizado	

12	Análisis de tráfico	
13	Repudio	
14	Escapes de información Interceptación de información (escucha)	
15	Alteración de la información Modificación de la información	
16	Introducción de información incorrecta	Introducción de falsa información
17	Degradación de la información	Corrupción de la información
18	Destrucción de información	Destrucción la información
19	Divulgación de información	Divulgación de información
20	Vulnerabilidades de los programas (software)	
21	Errores de mantenimiento / actualización	
22	De programas (software)	
23		Manipulación de programas
24	Errores de mantenimiento/ actualización de equipos hardware	
25	Caida de los sistemas por agotamiento de recursos.	
26		Robo
27		Ataque destructivo
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Ingeniería social

2.7 Riesgo residual

Para la valoración del riesgo residual se empleo un método cuantitativo en el cual se expresa de una manera subjetiva un nivel de valoración para determinar el impacto de la frecuencia y la valoración que se le da a los activos y elementos importantes para este proceso de análisis de riesgos.

Frecuencia: la escala de valoración que se empleo va desde 1 hasta 5, siendo 5 el mayor valor que se le puede dar a un evento que ocurre de una manera muy frecuente, el 1 se le otorga a un evento que ocurre con una frecuencia muy lejana es decir es poco probable que ocurra:

Tabla 2. 39 Valoración de la frecuencia

Valoración	Descripción de la frecuencia
5	Ocurre una vez al día.
4	Ocurre una vez a la semana.
3	Una vez al mes.
2	Una vez al año.
1	Intervalos superiores a un año.

Impacto: de manera similar se clasifica y se valora el impacto en un escala de 1 a 5, donde 5 es el máximo valor que se le puede dar a los deterioros y daños causados por dicho impacto y uno de la menor escala donde es el menor valor que se le puede dar el

impacto y las consecuencias que trae para el funcionamiento del sistema.

Tabla 2. 40 Valoración del impacto

Valoración	Descripción del impacto
5	Nivel alto.
4	Moderado.
3	Medio.
2	Bajo.
1	Insignificante.

2.7.1 Controles o medidas de protección encontradas

Para contrarrestar posibles situaciones, se mantienen medios y mecanismos para lograrlo, pero dichos mecanismos no se encuentran documentados ni están claramente definidos por tal razón para esta parte se tiene que definir que no se cuenta con mecanismos como tal. Al igual que la frecuencia y el impacto se determinó una escala en la cual se tomaron valores que van de 5 a 1, tabla 2.41, siendo 5 el valor que se que se le da al control que genera la máxima eficacia es decir un control el cual permite solventar de una manera eficiente o completa las posibles situaciones que se presentan.

Tabla 2. 41 Valoración de las medidas de protección

Valoración	Efectividad
5	Alto.
4	Moderado.
3	Medio.
2	Bajo.
1	Ninguno.

Controles existentes en el Centro de Datos.

Actualmente no tiene documentados los controles que aplican para garantizar la seguridad de la información, es decir las personas que se encargan de la administración las conocen y las aplican, en la tabla 2.42 se puede observar las mas trascendentales, para información adicional remitirse al anexo “Controles y políticas de seguridad existentes en el Centro de Datos”, que son los que actualmente se están aplicando.

Tabla 2. 42 Controles existentes

Activos	Controles	efectividad
Servicios	Acceso externo: para esto se manejan reglas de acceso para evitar accesos no permitidos en puertos abiertos.	Alta

	Correo no deseado: esto se realiza con el establecimiento de reglas en los equipos encargados de analizar los correos entrantes	Media
	Uso aplicaciones no permitidas: para esto se emplea un conjunto de reglas definidas en el administrador de ancho de banda con el fin de bloquear y asignar diferentes prioridades de acceso	Alta
	Actualmente los equipos principales tienen implementado un conjunto de reglas de iptables que permiten controlar posibles ataques de fuerza bruta o denegación de servicio.	Alta
Datos	Los datos de diferentes perfiles de usuarios se encuentran separados: tienen un equipo destinado a los datos de docentes y otro destinado para los estudiantes. Usuarios diferentes al administrador del sistema tienen privilegios restringidos para manipulación de información: para esto se emplean aplicaciones como scponly que permite crear usuarios que solo pueden acceder a los archivos de su directorio personal.	Media
	Los usuarios cuentan con una capacidad limitada en su directorio personal. Actualmente los usuarios no tienen acceso por shell a la información mantenida en los servidores.	Media
	Se manejan un sistema de copias de respaldo en el FTP, las copias se realizan de la información referente a la bandeja de entrada de los correos y el directorio personal de cada usuario, ese proceso se realiza en la noche. Esta información es borrada en un tiempo corto ya que no se tiene capacidad para almacenarla por más tiempo.	Media
	Aplicaciones informáticas Actualmente se realiza actualización de seguridad a los servidores: la actualización se realiza de forma manual el administrador del sistema quien la realiza al sistema operativo y a aplicaciones que lo permiten. El software se mantiene actualizado con versiones estables y recientes. Se cuenta con medios físicos que contienen el software necesario para los sistemas que actualmente se tienen en funcionamiento.	Alta
Hardware	Algunos equipos cuentan con redundancia de algunos de los elementos importantes para su funcionamiento: • Fuente potencia dual. • Dos interfaces de red. • Discos duros.	Alta
	El servidor de autenticación y enrutamiento se encuentra en redundancia	Alta
Personal	El acceso del personal a los servidores se tiene controlado	Media
	Medios de transporte de información seguros y cifrados empleando aplicaciones como SSHv2	Alta
	Para el establecimiento de contraseñas en los servidores se mantiene un esquema que permite establecer de una manera segura, para esto se tiene las contraseñas tienen superiores a 12 caracteres que deben ser numéricos y alfa numéricos, deben realizar una mezcla entre letras mayúsculas y minúsculas no deben corresponder a palabras que puedan ser encontradas en diccionarios.	Alta
Instalaciones	EL acceso del personal a las instalaciones se tiene restringido por: llave, Alarma Permiso previamente el diligenciado y entregado al vigilante de turno.	Media
	El ingreso personal ajeno al Centro de Datos se realiza bajo supervisión del administrador o de los monitores.	Alta
	Se encuentran vigilados y monitorizados con alarma	Alta
Equipamiento auxiliar:	Sistema de tierras para protección contra sobre voltaje. Se cuenta con un extinguidor pequeño	Media
Redes de Comunicación	No se tiene establecido ningún control. No se tienen equipos en redundancia.	Baja

Teniendo estos elementos se puede valorar y determinar un valor de riesgo residual para determinar la calidad y la necesidad de implantar nuevos controles que limiten los riesgos y daños que se pueden generar los elementos más importantes para el Centro de datos.

En la tabla 2.43 se muestra el cálculo de riesgo residual para las amenazas que se tienen actualmente, estas se definen de acuerdo a las más probables respecto a los elementos con los que cuenta el Centro de Datos.

Frecuencia = f
Impacto= I
Riesgo residual = RR
Efectividad = E
Nivel de Riesgo = NR

Tabla 2. 43 Riesgo residual respecto a las posibles amenazas

Tipo de amenaza		**f**	**I**	**NR**	**Control**	**E**	**RR**
Desastres naturales	Fuego	1	5	5	Extinguidor	2	2.5
	Daños por agua	1	5	5	Ninguno	1	5
Origen industrial	Contaminación electromagnética	1	1	1	Ninguno	1	1
	Averías de tipo físico y lógico	2	3	6	Cambios reemplazo	4	1.5
	Corte suministro eléctrico	3	4	12	UPS	3	4
	Condiciones inadecuadas de humedad	1	3	3	Ubicación instalaciones	4	0.75
	Fallos en los servicios de comunicaciones	3	4	12	Se cuenta con redundancia	5	2.4
	Interrupción de los suministros y servicios esenciales	2	3	6	Ninguno	1	6
	Degradación de soportes de almacenamiento de información	1	5	5	Cintas de respaldo	5	1
Errores y fallos no intencionados	Errores de administrador	2	5	10	Ninguno	1	10
	Error de usuarios	5	3	15	Copias respaldo	5	3
	Error de registros monitorización	1	1	1	Ninguno	1	1
	Error de configuración	2	4	8	Ninguno	1	8
	Difusión de software dañino	4	4	16	Antivirus	4	4
	Errores de re-encaminamiento	1	4	4	Ninguno	1	4
	Errores de secuencia	1	4	4	Ninguno	1	4
	Escapes de información	1	4	4	Ninguno	1	4
	Alteración de la información	1	5	5	Ninguno	1	5
	Introducción de información incorrecta	1	4	4	Ninguno	1	4
	Degradación de la información	2	4	8	Permisos restringidos	3	2.7
	Destrucción de la información	2	5	10	Copias de respaldo	3	3.3
	Vulnerabilidad de programas	3	5	15	Parches y actualizaciones	4	3.7
	Errores de mantenimiento y actualización de programas	2	5	10	Ninguno	1	10
	Caída del sistema por agotamiento de recursos	1	5	5	equipos redundantes	4	1.2

	Indisponibilidad del personal	1	3	3	suficiente personal	4	0.75
Ataques intencionados	Manipulación de la configuración	2	5	10	Ninguno	1	10
	Suplantación de la identidad	1	5	5	Ninguno	1	5
	Abuso de privilegios de acceso	2	5	10	Permisos restringidos	3	3.3
	Uso no previsto						
	Difusión de software dañino	3	4	12	Antivirus y parches	3	4
	Alteración de secuencia	2	4	8	Información cifrada	4	2
	Re-encaminamiento de mensajes	2	4	8	Ninguno	1	8
	Acceso no autorizado	3	5	10	Medios seguros	4	2.5
	Análisis de trafico	2	4	8	Trafico cifrado	4	2
	Repudio	1	4	4	Ninguno	1	4
	Interceptación de información	1	4	4	Ninguno	1	4
	Introducción de falsa información	2	5	10	Ninguno	1	10
	Corrupción de la información	2	4	10	Ninguno	1	10
	Divulgación de la información	1	4	4	Ninguno	1	4
	Manipulación de programas	3	4	12	Firewall	5	2.4
	Denegación de servicios	3	5	15	Firewall	4	3.7
	Robo	1	4	4	Control acceso	4	1
	Ataque destructivo.	1	5	5	Ninguno	1	5
	Indisponibilidad del personal	1	5	5	Ninguno	1	5
	Ingeniería social	1	4	4	Ninguno	1	4

Calculo del riesgo Residual con respecto a los activos, realizado de una manera global.

Valoración = V

Frecuencia Incidente = FI

Impacto = I

Nivel de riesgo = NR

Eficacia = E

Riesgo Residual = RR

Tabla 2. 44 Riesgo residual respecto a los activos

Activo		V	FI	I	N R	Controles	E	R R
Servicios	Web	10	3	1	3	Ninguno	1	3
	Proxy	8	3	2	6	Redundancia	4	1.5
	Correo	9	3	3	9	Redundancia	4	2.25
	DHCP	3	2	1	2	Ninguno	1	2
Datos	Configuración	10	2	5	10	Ninguno	1	10
	Administración	10	2	4	8	Ninguno	1	8
	Educativos	9	2	4	8	Realizan Copias	5	1.6
	Personales	8	3	3	9	Copias de los últimos meses	4	2.25
Software	Aplicaciones Unicauca	9	3	5	15	Ninguno	1	15
	Aplicaciones servicios	9	2	5	10	Ninguno	1	10
Hardware	Servidores	9	2	5	10	Ninguno	1	10
	Equipos de red	8	1	5	5	Ninguno	1	5
Recursos comunicaciones		8	2	4	8	Redundancia	4	2
Soportes Información		5	1	3	3	Redundancia	5	0.6
Equipamiento auxiliar		6	2	3	6	Ninguno	1	6

Instalaciones	9	1	5	5	Ninguno	1	5
Personal	10	2	4	8	Varios administradores	4	2

2.7.2 Análisis del riesgo residual

El riesgo residual, permite determinar la exposición de los elementos, se observa que en cuanto sea más alto el nivel de riesgo o la valoración que se encuentre, va ser más necesario el empleo de mecanismos y medios para controlar estos elementos. Del análisis anterior se encuentra necesaria la implantación de mecanismos para evitar amenazas las cuales pueden afectar los activos. Así mismo se encontró que algunas amenazas no son susceptibles a ser atendidas ya que los controles que existen son suficientes. Es importante denotar que todas las amenazas no pueden ser cubiertas ya que la implementación de estos mecanismos puede generar excesivos costos los cuales no se verán reflejados en un beneficio que pueda percibir el Centro de Datos y la comunidad universitaria que hace uso de los servicios del mismo.

2.8 Resultados de la etapa inicial

Del análisis anterior se puede concluir que se ha venido trabajando y emplea mecanismos de control y seguridad que hasta el momento han sido efectivos para las posibles situaciones que se han presentado, pero dichos mecanismos se realizan de manera manual y en ocasiones no se encuentran documentados o actualizados por tal razón:

- Es susceptible a que en un momento inesperado suceda una situación anormal que ponga en riesgo la correcta prestación de los servicios ofrecidos, y a la cual no se pueda responder de una manera efectiva ya que no cuenta con mecanismos definidos de manera clara y precisa y los cuales puedan generar resultados mucho más cortos y efectivos.
- Por otro lado no contar con un plan de continuidad del negocio que le permita afrontar situaciones de riesgo o situaciones que al ir cambiando necesiten irse actualizando, corre el riesgo de quedar relegado o atrasado ya que no se podrá ofrecer el nivel de servicio adecuado con respecto a los servicios.
- No se tiene un conocimiento de la legislación que cubre a esta área, o al tenerse un conocimiento parcial se corre el riesgo de caer en posibles situaciones ambiguas o

situaciones que pueden llevar a problemas legales por la falta de conocimiento de las mismas.

- El Centro de Datos cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas, por lo tanto se consideran no existentes, por tal razón se tienen deficiencias en cuanto al manejo de la seguridad de la información. Lo cual implica que se tengan falencias y que muy seguramente se dejen abiertas brechas de seguridad que en cualquier momento pueden afectar los servicios prestados.
- No se tiene definido quien maneja la seguridad de la información, estas actividades las realizan las personas encargados de la administración de los servicios, lo que ocasiona que se haga de manera empírica y con cierta regularidad pero no con la debida, ya que en ocasiones se realiza cuando hay situaciones que comprometen el funcionamiento de los mismos.
- No se tiene una clasificación de los activos, por tal razón no se ha priorizado el nivel de valor e importancia de los activos de información, de tal manera que se pueda llegar a tener controles efectivos de seguridad.
- No se ha realizado un análisis global o estándar de los posibles riesgos que podrían afectar la prestación de los servicios, para esto no es necesario un análisis técnico de cada servidor puerto por puerto, es mejor realizar un análisis estándar de los posibles fallos de seguridad que harán eco en la prestación de los servicios.
- El personal encargado de la seguridad de la información se capacita en el tema de manera autodidacta, pero una preparación más efectiva permitirá ofrecer una mejor respuesta ante posibles situaciones de riesgo que afecten la continuidad del negocio.
- Se puede determinar que el Centro de Datos requiere de un análisis de riesgos donde se puedan determinar los elementos más importantes para que este preste los servicios a la comunidad, donde se puedan identificar los activos más relevantes, se puedan priorizar y se puedan tener claramente definidos. Así mismo se pueda realizar una valoración de las amenazas que con mayor fuerza podrían afectar el funcionamiento y con esta información junto con el desarrollo de este proceso se puedan implementar mecanismos para mitigar estos riesgos y se puedan diseñar políticas de seguridad y un plan de contingencia que permita estar preparado para situaciones de riesgo que están presentes.

3. Guia metodológica para establecer los criterios para el diseño de políticas de seguridad para enfrentar los riesgos de seguridad a los cuales se encuentra avocado el Centro de Datos de la Universidad del Cauca.

3.1 Presentación

La presente guía metodológica para la realización de las políticas de seguridad del Centro de Datos de la Universidad del Cauca, esta basada en la guía metodológica general para una institución de carácter educativo propuesta en el anexo cuatro del presente trabajo de grado, es de aclarar que se realizaron todos los puntos que se consideraron aplicables en este caso y se revisaron otros que ya se encontraban desarrollados, implementados o considerados con anterioridad por el personal del Centro de Datos.

Por lo anterior en el presente documento se presentan las consideraciones tomadas en cuenta de la guía general, junto con resultados y consideraciones hechas de acuerdo al orden establecido en dicha guía, de forma tal que sirva de referente para la un próximo trabajo de actualización de políticas para el Centro de Datos o procesos de revisión de las mismas.

3.2 Introducción

La prestación de los servicios del Centro de Datos de la Universidad del Cauca es de vital importancia para su desempeño tanto de la parte administrativa como de la académica, el que hacer de la Universidad en varios de sus campos de acción como el investigativo, el financiero, la docencia, su avance e impacto con nuevos proyectos, se basa fuertemente en la funcionalidad de su Centro de Datos, debido a esta importancia se debe pensar en la seguridad informática, ya que esta se ve cada vez más amenazada por el desarrollo de nuevas tecnologías, plataformas de computación, la interconexión mundial de redes, amenazas que pueden afectar la prestación de los servicios y por ende a toda la comunidad educativa en general.

Esto lleva a la creación de directrices para el uso adecuado de las tecnologías y

recomendaciones para obtener el máximo beneficio de ellas en la institución por parte de toda la comunidad universitaria, las políticas de seguridad se dan como una herramienta de tipo organizacional para contribuir en esta problemática y lograr concienciar sobre la importancia y sensibilidad de la información y de los servicios críticos para la Universidad mantenerse como pionera en su campo de acción.

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

Para la creación de las políticas se llevaron a cabo las cuatro fases planteadas por la guía metodológica general, siguiendo la serie de criterios establecidos de manera secuencial.

3.3.1 FASE I. Inicio

Etapa de referencia I. Conformación de un equipo de trabajo

Se conformó el equipo de trabajo teniendo presente los perfiles de cada persona para los roles sugeridos en la guía metodológica, como se puede apreciar en la figura 3.1 creada con *Word*:

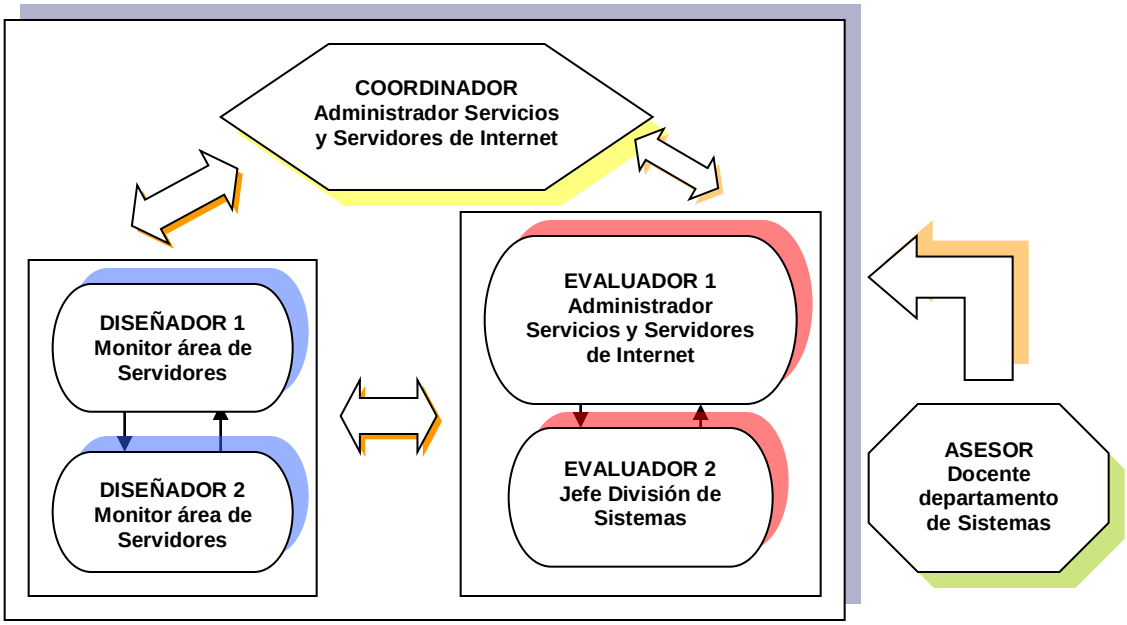


Figura 3. 1 Equipo de trabajo creación de políticas de seguridad

- **Coordinador:** Ing. Jaime Andrés Gaviria. Administrador Servicios y Servidores de Internet Universidad del Cauca.
- **Diseñador 1:** Fabián Andrés Mera. Monitor área de Servicios y Servidores de Internet Universidad del Cauca.
- **Diseñador 2:** Carolina Guevara Campo. Monitora área de Servicios y Servidores de Internet Universidad del Cauca.
- **Evaluador 1:** Ing. Jaime Andrés Gaviria. Administrador Servicios y Servidores de Internet Universidad del Cauca.
- **Evaluador 2:** Ing. Maria Clara Rodríguez. Jefe división de Sistemas Universidad del Cauca.
- **Asesor:** Ing. Siler Amador Donado. Docente departamento de Sistemas Universidad del Cauca. Director del trabajo de grado.

Lo referente a la representación de la parte legal se manejo con la oficina jurídica de la Universidad con la presentación a esta, del documento de políticas de seguridad de la información realizado y revisado por el presente equipo de trabajo, para que procedan a su estudio acorde con los reglamentos y estatutos que rigen a la Universidad, con el fin de considerar el incluir las políticas en estos reglamentos.

Etapa de referencia II. Conocimiento teórico sobre políticas de seguridad

Todos los integrantes del equipo de trabajo debido a su formación profesional ya poseen nociones generales sobre la seguridad de la información, por lo que se consideraron no oportunas las evaluaciones, además que de acuerdo al rol específico de cada uno, poseen los conocimientos suficientes y necesarios para cumplir con sus funciones.

NOTA:

Si el equipo de trabajo realiza cambios en su conformación, debe dirigirse a la guía general para revisar todos los puntos planteados por esta y así mantener las caracteristicas requeridas del equipo para realizar un adecuado trabajo sobre las políticas de seguridad.

Etapa de referencia III. Realización de un análisis de riesgos

Realizado satisfactoriamente acorde con el anexo de la guía metodológica general, su desarrollo y resultados se encuentran en el capitulo dos del presente trabajo de grado, con toda la información y documentos generados por este proceso para poder continuar con la fase dos, con el análisis de riesgos se logro la clasificación y control de activos, detectar y valorar todos los riesgos que amenazan la estabilidad y seguridad en el Centro de Datos, lo cual permite establecer las políticas de seguridad de la información de una manera mas acertada y optimizada.

NOTA:

Es importante recordar que el proceso de análisis de riesgos debe realizarse cada determinado periodo de tiempo, debido a los cambios que surgen en la institución, así como las crecientes amenazas.

Etapa de referencia IV. Consideración de aspectos que moldean las políticas

Se tuvieron presentes los siguientes criterios de la tabla 3.1 para este fin:

Tabla 3. 1 Criterios para establecer políticas de seguridad

Criterios	Aplicación
Caracteristicas de las políticas:	• Reflejan sus objetivos. • Contienen una descripción clara de los elementos involucrados en su definición. • Ofrecen explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones. • Se busca transmitir por qué son importantes éstos u otros recursos o servicios. • Manejo de un lenguaje claro.
Acciones pro-activas.	• Se tiene presente el historial de fallos. • Se consideran todos los riesgos que se consideraron posibles.
Conciencia de seguridad.	• A través de conferencias al personal.
Políticas obvias.	• Se tienen en cuenta las acciones que se consideran obvias.
Tratar la seguridad con independencia y objetividad.	• Contando con la revisión de todo el equipo de trabajo.

Como se puede observar en la figura 3.5, creada con la utilidad gráfica de *Word,* se

cumplió con el flujo de etapas y gracias a los resultados obtenidos se puede continuar con la fase 2.

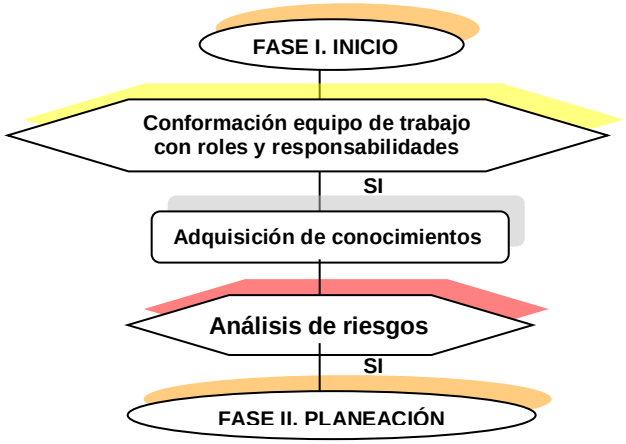


Figura 3. 2 Etapa de inicio

3.3.2 FASE II. Planeación

Entradas: los resultados de la fase de inicio, equipo de trabajo, documento análisis de riesgos.

En la tabla 3.2 se encuentran las etapas de referencia seguidas para lograr el objetivo de la fase:

Tabla 3. 2 Etapas fase de planeación

Etapa	Desarrollo
Establecer el alcance de políticas.	Las políticas de seguridad serán planteadas y diseñadas únicamente para los elementos y servicios que son soportados por el Centro de Datos de la Universidad del Cauca.
Involucrar a toda el área propietaria de los recursos o servicios.	Por las características del proyecto y su alcance no se involucra en el proceso a todo el personal del Centro de Datos, solo el Administrador de los servicios y dos monitores.
Establecimiento de una comunicación eficaz.	Esta se establece a través de correo electrónico, informes digitales y escritos, entrevistas y reuniones previamente definidas.
Establecer las interrelaciones necesarias.	Se pactan reuniones con el área de infraestructura que tiene acceso al Centro de Datos.

En la tabla 3.3 se encuentran los criterios tenidos en cuenta en esta fase:

Tabla 3. 3 Criterios fase de planeación

Criterio	Aplicación
Apoyo y compromiso de la	Se cuenta con el apoyo y el aval del Administrador de los servicios

parte administrativa.	encargado de los servidores y servicios para los cuales se crean las políticas, así como el del jefe de la división de sistemas.
Autoridad en las decisiones.	Para la definición y planeación se requiere de la aprobación del asesor y para la implementación del coordinador del equipo.
Considerar estándares de seguridad de la información.	Se toman como referencia los estándares ISO 17799 e ISO 27001.
Análisis de requerimientos de seguridad informática.	Establecimiento de un nivel de seguridad aceptable: en una escala de 1 a 5 para el nivel de seguridad, se considera aceptable una medida de 4 (bueno), la cual se logrará con la implementación de las políticas de seguridad en un porcentaje igual o superior al 80%. 1 Malo, 2 Regular ,3 Aceptable, 4 Bueno y 5 Excelente.
Aseguramiento de los datos (confidencialidad, integridad, disponibilidad).	Durante la elaboración de las políticas se han tenido presentes estos tres aspectos de la información.

Debido al cumplimiento de las etapas de referencia de esta fase, así como la consideración de los criterios se puede continuar el flujo de trabajo hacia la etapa de establecimiento:

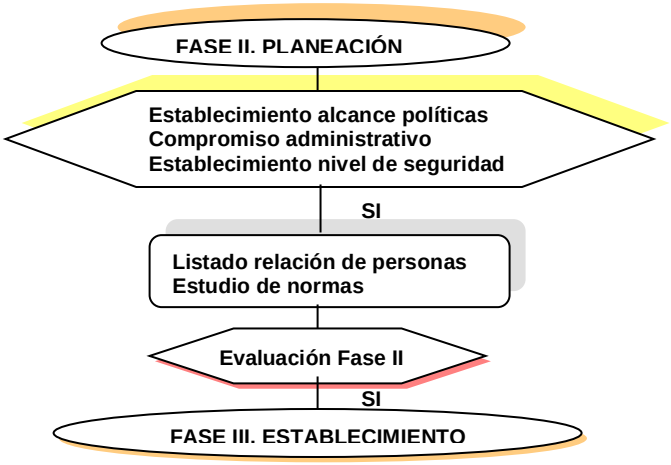


Figura 3. 3 Fase de planeación

3.3.3 FASE III. Establecimiento

Entradas: los resultados de la fase de planeación.

Resultado: Documento con las políticas de seguridad.

En la tabla 3.4 se encuentran los criterios considerados para la creación de las politicas, con base en las áreas de seguridad establecidas por la norma ISO 17799:

Tabla 3. 4 Criterios con base en las áreas de seguridad de la ISO 17799

Criterio	Aplicación
Política de seguridad.	Se consignan las políticas en un documento escrito.
Clasificación y control de activos.	Se realiza en el análisis de riesgos.

Seguridad organizacional.	Se crearon políticas para revisiones y actualizaciones.
Aseguramiento del componente humano.	Se considera un aparte relacionado exclusivamente al personal.
Aseguramiento de la infraestructura física.	Se establecieron apartes para hardware, instalaciones, equipamiento auxiliar.
Control de accesos.	En todos los apartes de las políticas se incluye el control de accesos.
Continuidad de las operaciones de la organización.	Se logra con la creación del plan de contingencia, así como el cumplimiento de varias políticas que lo estipulan.
Aseguramiento de los componentes de ínter conectividad.	Se encuentran en el aparte de redes de comunicaciones.
Aseguramiento de los componentes software y hardware.	Se encuentran en el aparte hardware, información y utilización de los servicios.
Requerimientos legales.	El documento de políticas de seguridad se sometió a la revisión por parte de la representante legal de la Universidad.

Como complemento a los anteriores puntos se realizaron las siguientes etapas de referencia:

Tabla 3. 5 Etapas de referencia fase de establecimiento

Etapa	Desarrollo
Definición de violaciones y de las consecuencias del no cumplimiento de la política.	Se establecen sanciones para el no cumplimiento de estas.
Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.	En varias de las políticas se ven estos aspectos, por ejemplo en los requerimientos para la prestación de los servicios.
Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.	En varias de las políticas se ven estos aspectos, por ejemplo en las referentes a la creación de cuentas.
Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.	En varias de las políticas se ven estos aspectos, pueden verse en las de prestación de los servicios, archivos de configuración.
Informar a todos los involucrados.	Se ve reflejado en las políticas y en la entrega de resultados e informes.

Todos los puntos sugeridos en esta fase de establecimiento han sido tenidos en cuenta para la elaboración del documento de políticas de seguridad, el cual se encuentra en el capitulo 4 del presente trabajo de grado.

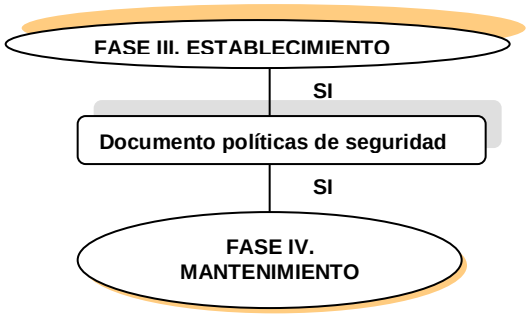


Figura 3. 4 Fase de establecimiento

3.3.4 FASE IV. Mantenimiento

Entradas requeridas: el documento de políticas de seguridad.

Para todos los puntos sugeridos en esta parte se crearon políticas de seguridad que los contemplan, como lo son el establecimiento de revisiones, actualización en la información de seguridad, administración, monitoreo y reporte de sucesos, establecimiento de un sistema de medición para evaluar el desempeño de las políticas y el establecer procesos de actualización periódica de las políticas sujetas a los cambios organizacionales relevantes.

Debido a la realización de todas las fases con sus respectivas etapas de referencia, así como la consideración de todos los criterios dados se logra el objetivo último de la guía que es el documento de políticas de seguridad de la información para el Centro de Datos de la Universidad del Cauca.

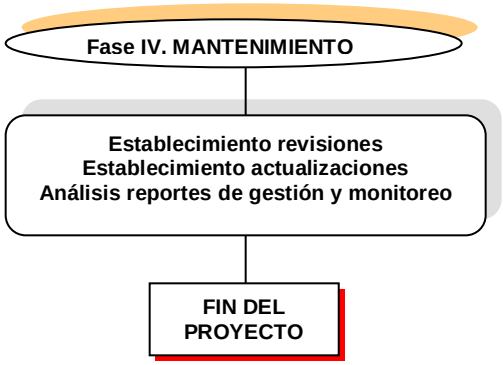


Figura 3. 5 Fase de mantenimiento

3.3.5 Cronogramas de referencia

Para la realización de la guía metodológica el cronograma sugerido se adaptó al desarrollo del presente trabajo de grado.

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

El desarrollo de este se puede observar paso a paso en el capítulo dos del presente trabajo de grado.

4. Políticas de seguridad para el Centro de Datos

El presente documento contiene las políticas de seguridad creadas para el Centro de Datos de la Universidad del Cauca, divididas en una sección para los usuarios y otra para los administradores, separadas de esta manera porque se considero que es una mejor forma de presentación y organización.

4.1 Políticas de seguridad para los administradores del Centro de Datos

Dentro del planteamiento de las políticas de seguridad se realizan una serie de recomendaciones en caso de infracción a las políticas estipuladas en el presente documento, pero al presentarse una falta o violación a una de las políticas aquí establecidas se aclara que está sujeta a las sanciones o amonestaciones declaradas en los respectivos reglamentos internos que se manejen. Estas recomendaciones se consideran oportunas de ser estudiadas por el ente legal para ser incluidas en los reglamentos.

La administración de los servicios la realizan el administrador de los servicios y los monitores del área, los cuales tienen las funciones de velar por la integridad de los servicios y garantizar su óptimo funcionamiento, así mismo se encargan de realizar el mantenimiento preventivo de los equipos, las instalaciones y los servicios que se prestan.

Políticas generales:

Prestación de los servicios: Utilización de aplicaciones

1. Se debe restringir el uso de aplicaciones que afecten el rendimiento general de la red para los fines universitarios, velando sobre todo el cumplimiento de ello en los horarios laborales.
2. Para las transacciones en línea que realiza la Universidad del Cauca se deben tomar todas las medidas pertinentes a proteger dichas transacciones como lo son evitar

interrupciones, mensajes no autorizados, alteraciones de la información, accesos no autorizados, duplicación o repeticiones, etc.

Administración de los servicios:

3. Establecer planeaciones para la actualización y mejoramiento de los servicios.
4. Mantener una revisión permanente de los servicios, de tal manera que se pueda monitorear y llevar un consolidado de información y rendimiento de los mismos.
5. Establecer indicadores para medir la eficacia y la calidad de los servicios.
6. Cuando un servicio sale de funcionamiento se debe restaurar el mismo en el menor tiempo posible y se debe disponer de todos los insumos para garantizar un tiempo mínimo de reestablecimiento.
7. Establecer mecanismos para actualización y mejora de los servicios con los que se cuenta. Revisiones periódicas de mejoras o nuevas versiones en los servicios prestados.
8. Analizar y programar revisiones para instalación de parches de seguridad, antes de realizarlo se debe realizar una copia de la última versión buena conocida del archivo de configuración y del paquete actual completo.
9. Para realizar cambios en las aplicaciones y los servicios se debe contar con el aval del administrador de los servicios.
10. Los servicios no deben ser detenidos o reiniciados sin previo aviso, se debe realizar con una fecha programada, con el fin de evitar pérdidas o situaciones imprevistas, salvo casos de fuerza mayor que serán determinados por el administrador de los servicios.
11. Los servicios deben ser mantenidos y suministrados solo por la persona autorizada, a las consolas de administrador y a los archivos de configuración de los servicios y del sistema no se puede acceder con un usuario diferente.
12. Cuando un servicio presenta un mal funcionamiento se debe mirar la causa y si es por algún cambio realizado recientemente en los archivos de configuración o en el paquete en sí deben ser actualizados o reemplazados por uno bueno conocido.
13. Mantener un cronograma de revisiones y de cambios en los archivos de los servicios de tal manera que se preste un óptimo servicio.

Mantenimiento de los servicios: instalación, configuración:

14. Realizar un proceso de estudio antes de la instalación o configuración de servicios, analizando su factibilidad y viabilidad para la decisión de implementarlo.
15. Instalar y configurar un nuevo servicio en un equipo de prueba, después de verificado su correcto funcionamiento migrarlo al servidor final.
16. Al realizar cambios de fondo en los servicios mantener un equipo de respaldo hasta verificar por un periodo prudente el correcto funcionamiento del actual.

Políticas específicas de los servicios:

Políticas para el uso de correo electrónico:

17. El servicio de correo cuenta con una capacidad y un límite de almacenamiento determinado, se debe velar porque no se sobrepase dicho límite, para lo cual se pueden establecer tiempos de gracia que después de ser superados se procederá a informar al usuario con el fin de lograr mantener la capacidad establecida como límite.
18. Se deben realizar copias de respaldo del correo electrónico y de los archivos de las cuentas personales, estas copias deben mantenerse por un tiempo prudente en el cual se pueda recuperar la información cuando suceden situaciones imprevistas.
19. Los usuarios deben contar con una carpeta denominada Posible *Spam* en la que encontraran los correos que han sido clasificados como tal, estos correos se deben mantener en esta capeta por un tiempo 15 días, en los cuales automáticamente serán eliminados de los servidores.
20. Caducidad de las cuentas de correo. Estas son de carácter indefinido, pero la no utilización de ellas por un período de seis meses conllevará a su suspensión y pasado un año a su eliminación de los servidores de correo.

Políticas para el uso del servicio de navegación por Proxy

21. Por defecto cualquier miembro de la comunidad universitaria puede acceder a este servicio.
22. Se debe velar porque el servidor Proxy no sea utilizado para correr aplicaciones que

son catalogadas como p2p.

23. Cuidar de que el servidor Proxy no sea empleado para pruebas de aplicaciones que pueden generar mal funcionamiento de la red.
24. Cuando se requiere el acceso a un sitio especifico el cual se encuentra bloqueado por el Proxy, se debe recibir una solicitud formal dirigida al administrador de los servicios indicando la necesidad de habilitar el acceso al puerto especifico, adjuntando en el mismo la justificación correspondiente.
25. Se deben establecer mecanismos para la regulación del consumo del ancho de banda y la optimización de la velocidad de acceso a Internet para sitios y aplicaciones importantes para la comunidad universitaria.

Políticas para el uso del servicio Ftp:

26. Para crear una cuenta en el servidor FTP se debe contar con un oficio dirigido al administrador de los servicios y se debe contar con los siguientes requisitos: ser docente o administrativo o director de un grupo de investigación reconocido y avalado por la Universidad del Cauca, sustentar en la carta la necesidad de utilización de una cuenta ftp y especificar el tipo de información a ser alojada en este servidor.
27. Contar con los datos personales del responsable del sitio a crear.
28. El servidor ftp pueden ser accedido de manera anónima, es decir, puede ser accedido por cualquier persona para descargar información de interés que encuentre en este sitio, sin ningún tipo de restricción.
29. No se debe publicar contenido de tipo pornográfico o contenido que sea lesivo contra una institución o una persona.
30. No se debe publicar software que tenga algún tipo de restricción o del cual no se tenga la licencia respectiva para la distribución y difusión. El software que puede ser publicado debe estar regido bajo una licencia de libre distribución.
31. La cuenta creada para un usuario o grupo de investigación tiene una capacidad máxima de almacenamiento, la cual debe ser tenida en cuenta para controlar que no sea sobrepasada.
32. La cuenta será enjaulada para prevenir accesos no autorizados a la información de otros usuarios.

Políticas para el servicio hosting y el de base de datos

33. Para crear un sitio Web se debe tener un oficio en cual se consigne: la importancia y la necesidad de contar con un espacio Web, el contenido que será publicado, el responsable de administrar y mantener el contenido, el tipo de aplicación que se empleará para administrar y mantener la información, asimismo indicar si requiere la utilización de bases de datos.
34. Un espacio en el servidor Web para implementar un sitio o para brindar el servicio de hosting se asigna a una dependencia, facultad o departamento que haga parte de la Universidad y adicionalmente a los grupos de investigación que cuenten con el aval de un docente. También puede ser asignado a un administrativo que no vaya a ser uso del sitio como página personal.
35. La forma como se creará el nombre del sitio y la URL o dirección electrónica queda estandarizada y definida por: www.unicauca.edu.co/nombre_del sitio.

Servicio Web

36. El portal institucional es la cara visible de la Universidad del Cauca, por tal motivo es de suma importancia velar porque esté servicio se encuentre activo y en óptimas condiciones de funcionamiento.
37. Cuando ocurre algún tipo de inconveniente en el portal institucional que lo deshabilite o saque de funcionamiento se debe redireccionar a una página de mantenimiento donde se especifique que actualmente se encuentra fuera de servicio.
38. Si por algún motivo la página principal es vulnerada o sufre un ataque deliberado dicho incidente de ser registrado y reportado lo antes posible al administrador de los servicios y se deben tomar los correctivos necesarios que permitan retornar a condiciones normales.
39. Se debe cuidar en los servidores correspondientes a administrativos, docentes y estudiantes de la prestación del servicio Web para sus páginas personales.

Servicio de DHCP

40. Todos los usuarios tienen acceso y están habilitados para hacer uso del servicio de

DHCP, por lo que se debe velar por su óptimo funcionamiento.

Servicio Ras

41. El acceso a Internet por medio del servicio de acceso remoto se debe realizar de una manera controlada y responsable de tal manera que no afecte las labores y las funciones de los servicios.

Asignación de direcciones públicas y NAT

42. Para brindar el acceso a Internet con direcciones publicas, se debe contar con un oficio que relacione los siguientes datos: nombre del solicitante, cargo del solicitante, justificación del uso de la dirección y la aplicación que va a emplear, así como los datos del equipo en la cual esta dirección será asignada.
43. Sólo los docentes, grupos de investigación y administrativos que justifiquen la necesidad de uso, tendrán la posibilidad de que se les asigne una dirección.
44. Quedan prohibidas las aplicaciones P2P[11] en horarios laborales, ya que por sus características son un riesgo potencial para la red.
45. La descarga de información debe ser controlada y esta información debe tener un carácter educativo.
46. Las aplicaciones P2P o aplicaciones empleadas para hacer un mayor uso del ancho de banda deben usarse en los horarios permitidos y especificados por el área de servicios y servidores de Internet.

Políticas utilización de aplicaciones

47. Aplicaciones p2p: están totalmente prohibidas en horarios laborales, el uso de las mismas se debe justificar bajo un ambiente netamente educativo, su uso esta permitido en horarios no laborales y la responsabilidad por los inconvenientes que pueden causar estas aplicaciones recae sobre los usuarios que hacen uso de las mismas, por lo tanto ellos son los directos responsables de las incidencias y consecuencias que pueda traer, tanto para el usuario como para la red. En caso de

[11] P2P: conexiones par a par, las cuales son empleadas por programas de descargas que consumen gran cantidad de recursos de red.

incurrir en una falta contra esta política, el administrador de los servicios esta en la facultad de eliminar las conexiones presentes y de restringir o bloquear la dirección IP de la máquina que esta generando este tráfico, en caso de encontrarse de manera repetitiva, el administrador esta en la facultad de cancelar el uso de esta dirección, de tal manera que quede restringido de manera permanente.

48. Para el uso de aplicaciones punto a punto que requieren tener características de conexión altas y requieren de direcciones públicas o de NAT, se debe especificar la necesidad de la utilización de este tipo de aplicaciones y se debe sustentar la necesidad en el entorno académico, de tal manera que se pueda realizar la gestión necesaria para llevar a cabo este proceso. Se debe adjuntar en la información el nombre de la persona, el tipo de aplicación a emplear y el tiempo de uso de esta aplicación. Los puertos necesarios para emplear la aplicación y el destino de la conexión.
49. Aplicaciones de videoconferencia que requieren gran uso del canal. Para este tipo de aplicaciones se cuenta con equipos y con un direccionamiento especial el cual se debe asignar, de tal manera que para este tipo de eventos se pueda garantizar un ancho de banda lo suficientemente adecuado.

4.1.1 Información

Acceso a la información

50. Restringir el acceso de los usuarios a la información exclusiva de su propiedad.

Administración:

51. Los logs (archivos de bitácora) así como otros registros que almacenan los eventos importantes de seguridad de los sistemas deben ser revisados de forma periódica y guardarse durante un tiempo mínimo establecido, ya que estos archivos colaboran significativamente en la detección de intrusos, fallas de seguridad y otras actividades de auditoria. Deben ser protegidos y estar en un lugar que solo el personal del Centro de Datos pueda leerlos.
52. Establecer períodos de tiempo no superiores a tres meses para confrontar la

información actual de estos registros con los datos anteriores que relacionan este tipo de eventos, en lo posible emplear una herramienta que permita realizar este proceso.

53. No divulgar información confidencial a personas no autorizadas.

Seguridad de la información:

54. Garantizar la disponibilidad de los datos a sus respectivos propietarios en el momento que ellos lo requieran.
55. Velar por mantener la integridad de los datos.
56. Cerrar cualquier tipo de carpeta abierta o compartida que no sea necesaria o cuyo fin implique riesgos de seguridad.
57. Velar por la confidencialidad de la información cuidando de no permitir que esta sea vista y borrarla cuando ya no sea necesaria.
58. Transmitir la información confidencial y de uso restringido de una manera cifrada.
59. Cuando se realizan pruebas con información confidencial, esta debe ser debidamente protegida, de igual manera asegurarse de ser almacenada o eliminada al finalizar las pruebas.

Copias de la información:

60. Realizar copias de seguridad de la información de forma periódica, copias completas semanales e incrementales diariamente, así como una copia total de forma mensual.
61. Verificar la correcta recuperación de copias anteriores por lo menos una vez por mes si no se ha realizado con anterioridad.
62. Guardar en un sitio remoto a las instalaciones las copias de seguridad de los servidores.

Archivos de configuración

63. Los archivos de configuración sólo pueden ser accedidos y modificados por el usuario root o el usuario propietario del servicio, a esta cuenta sólo tiene permiso el administrador, esto es para los servidores montados sobre Linux. Para los servidores montados sobre Windows se utiliza únicamente la cuenta de administrador y solo

deben tener permiso para este usuario.

64. No pueden ser modificados sin previo aviso.
65. Cuando se realicen modificaciones en los archivos de configuración se debe mantener una copia previa del archivo que se está ejecutando actualmente para el funcionamiento del servicio.
66. De todos los archivos de configuración de los servicios que son soportados por el Centro de Datos, se debe mantener una copia de respaldo que garantice su pronta recuperación en caso de ser eliminados.
67. Las modificaciones que se realicen en los archivos deben ser previamente autorizadas y probadas en un servidor de respaldo.
68. No se pueden difundir copias de los archivos de configuración que actualmente se tienen corriendo en los servidores.
69. Las copias deben realizarse de manera manual o con un mecanismo que permita realizarlas de manera automática según se requiera.
70. Cualquier tipo de cambio o actualización a los paquetes de software debe realizarse con la debida autorización y supervisión del administrador de los servicios.

Información almacenada en bases de datos

71. Dicho información sólo puede ser accedida por el usuario propietario o la aplicación que hace uso de métodos para almacenar información.
72. Las cuentas para almacenar esta información cuentan con una capacidad máxima de almacenamiento.

Información almacenada en los espacios Web del servidor institucional

73. Los usuarios que tienen una cuenta en el servidor institucional, tienen autonomía de generar sus propios portales empleando aplicaciones como mambo[12], php[13], java Script[14] o HTML[15].

[12] Mambo: aplicación que permite generar sitios Web de manera dinámica.
[13] PHP: lenguaje de programación empleado para la creación de contenido para sitios Web.
[14] Javascript: lenguaje de programación orientado a objetos.
[15] HTML: hypertext Markup language; lenguaje de marcas hipertextuales empleado para la creación de contenido de sitios Web.

74. La información de estos portales es administrada totalmente por los usuarios propietarios.
75. Dicha información puede sólo ser accedida para ser modificada o eliminada por los usuarios propietarios de la misma.
76. Se debe realizar copias de respaldo periódicas de la información contenida en dicho servidor, de tal manera que se puedan realizar recuperación de la información cuando ocurren incidentes no previstos.
77. Los sitios, el mantenimiento de los mismos y la aplicación de parches son responsabilidad del propietario, así como las implicaciones que conlleve el no hacerlo.

Información referente a la documentación del área

Corresponde a la información necesaria para realizar la configuración de los servicios y los servidores con los cuales cuenta el Centro de Datos, esta información constituye un apoyo para el personal del área cuando suceden situaciones imprevistas que sacan de funcionamiento los servicios y deben ser reinstalados, así mismo es un apoyo cuando se necesita migrar a los equipos a nuevos sistemas operativos, nuevos servicios o versiones.

78. Esta información debe ser actualizada cada seis meses.
79. Cuando se realiza un cambio en la configuración de una aplicación o servicio, los cambios deben ser consignados en la documentación actual.
80. Las aplicaciones que se instalan deben contar con una documentación que respalde el procedimiento, de tal forma que en caso de presentarse una situación imprevista pueda ser empleada para retornar a su correcto funcionamiento.
81. Esta información no puede ser accedida por personas diferentes a los administradores de los servicios.
82. El formato de los documentos que contiene información de la configuración e instalación de los servidores y servicios debe ser mantenido.
83. Cualquier falla o inconsistencia en la misma debe ser corregida y actualizada.
84. Debe ser mantenida en un lugar en el cual pueda ser accedida fácilmente por los administradores.
85. Se deben documentar claramente los cambios realizados a los equipos.

Información personal de los usuarios

Es información referente a cada usuario, que cuenta con una cuenta de correo electrónico y con un espacio para tener su página personal.

86. La información de los usuarios cuenta con una determinada capacidad de almacenamiento, cuando se sobrepasa dicho límite el usuario queda imposibilitado para incrementar la capacidad para almacenar información en el servidor.
87. En casos especiales a los usuarios se les puede incrementar la capacidad de almacenamiento que se tiene, para esto requiere de una justificación y una aprobación del administrador de los servicios.
88. El correo y la información que es enviada por este medio no puede ser revisada por ninguna persona diferente al propietario, incluso está prohibido para el administrador verificar el contenido, en casos extraordinarios se tendrá esta posibilidad si se cuenta con el permiso del usuario para llevar a cabo dicha actividad.
89. Realizar copias de seguridad de forma automática cada ocho días de todo el contenido y diariamente de los cambios.
90. Las copias se almacenan en cintas y por un tiempo no superior a tres meses.
91. Para recuperar las copias se debe contar con autorización del propietario, quien manifestara esta necesidad por un medio escrito, solicitud telefónica o correo electrónico.
92. La información se recuperará en el espacio personal del solicitante, bajo una carpeta llamada recuperados, en la cual el solicitante verificara la información recuperada.
93. No se puede acceder a la información personal sin previa autorización del propietario.

4.1.2 Hardware

Acceso a los equipos

94. El acceso a los equipos hardware solo debe realizarse por el personal del área de servidores y servicios de Internet, en caso de requerirse por un tercero debe ser con la autorización expresa del administrador de los servicios.
95. Siempre que acceda personal externo se debe contar con la presencia de uno de los

miembros del área quien velará por el adecuado comportamiento del tercero.

96. Los servidores de red y los equipos de comunicación (*Switchs*, *Routers*, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robos. Debe restringirse severamente el acceso a estos lugares y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de inteligentes).

Administración de los equipos

97. Revisar semestralmente la adecuada utilización de los equipos de acuerdo a las necesidades de lo que estén soportando, para establecer cambios que mejoren la eficiencia en su uso.

Instalación, configuración y reemplazo

98. El hardware no debe ser cambiado sin previa autorización del administrador de los servicios, cuando se realizan cambios deben ser registrados.
99. Antes de realizar el cambio de algún dispositivo o elemento, se debe realizar pruebas de funcionamiento del mismo.
100. Los elementos hardware deben ser manipulados teniendo en cuenta los cuidados requeridos, así mismo empleando las herramientas y elementos necesarios.
101. Cuando falla un dispositivo se debe revisar la garantía, para realizar la respectiva devolución si aún se cuenta con ella.
102. Cuando falla un equipo importante se debe montar sobre un equipo de respaldo una replica del equipo que falla, para de esta manera evitar que el servicio salga de funcionamiento por un tiempo muy prolongado.

Planes de continuidad y contingencia

103. Establecer un plan de contingencia que cubra todas las necesidades del Centro de Datos.
104. Establecer revisiones periódicas del plan de contingencia, para verificar su funcionamiento y actualización.

Mantenimiento

105. Establecer jornadas semestrales de mantenimiento a los equipos hardware, en lo referente a actualización, reparación, limpieza y organización de estos elementos.
106. El mantenimiento debe ser realizado y programado de manera segura, de forma que no afecte las actividades que dependen del funcionamiento de estos equipos.
107. Se deben mantener los equipos y el hardware con las debidas protecciones para evitar problemas de seguridad.
108. Al realizar mantenimiento se debe tener en cuenta las piezas o elementos que se hayan deteriorado por el uso, para de esa manera establecer el reemplazo de elementos.

Servidores y equipos de red

Estos equipos son el núcleo principal de los servicios ya que sobre estas máquinas se encuentran alojados y corren las aplicaciones de software necesario que permiten que el Centro de Datos preste los servicios a la comunidad universitaria.

109. Cuando se realiza reemplazo de un elemento, este debe cumplir con las especificaciones técnicas que requieren el dispositivo.
110. Se debe realizar el mantenimiento preventivo de los equipos de red que hacen parte del Centro de Datos, con jornadas previamente definidas y que involucren al área de infraestructura.
111. Se deben garantizar las condiciones necesarias tanto para el sistema eléctrico como para el de refrigeración con el fin de evitar posibles daños de los equipos.
112. Los equipos que no son propios de la Universidad del Cauca y que se encuentran en comodato por las empresas proveedoras de servicio, no deben ser manipulados ni se les debe realizar mantenimiento ya que es obligación de la empresa proveedora realizar dichas actividades.
113. Las actividades de mantenimiento deben ser programadas con un tiempo de anticipación, en el cual se tengan en cuenta el calendario académico y otras actividades institucionales que se puedan interrumpir e informar de ellas a quien se

tenga conocimiento que pueda ser afectado por dicho mantenimiento.

Estaciones de trabajo

Son equipos adicionales de los administradores con funciones necesarias para gestionar y mantener los servicios que se prestan.

114. Todos los administradores deben contar con la contraseña para acceder con el usuario de mayor privilegio.
115. Cuando se desea realizar algún cambio de hardware, dicho cambio debe ser notificado al administrador de los servicios y debe ser registrado en las actas correspondientes para este fin.
116. Cuando se realiza un cambio mayor como cambio de sistema operativo se debe mantener las cuentas de usuarios de los otros administradores así como los archivos de contraseñas y configuración de servicios, para esa manera no generar traumatismos ni inconvenientes.
117. Estas estaciones de trabajo se pueden emplear como equipos de prueba antes de realizar las respectivas modificaciones en los servidores.
118. Los administradores son responsables por el funcionamiento de dichas estaciones y por las aplicaciones que en el se encuentran instaladas.
119. Se debe asegurar la robustez de las contraseñas de todas las cuentas en cada una de las estaciones, es decir la manera como se crean contraseñas.

4.1.3 Instalaciones

Corresponden a las instalaciones donde se encuentran alojados servidores y equipos de red, así como los equipos que proveen servicios adicionales para que el Centro de Datos pueda llevar a cabo su funcionalidad. En la sala donde actualmente se encuentra la mayor cantidad de equipos es el IPET. En estas instalaciones se encuentran alojados los servidores y equipos de red que conforman el núcleo de la infraestructura física del Centro de Datos.

Acceso a las instalaciones

120. El acceso a las instalaciones que alojan los servidores debe restringirse al personal del área.
121. En caso de requerir acceso de terceros involucrados se debe llevar un registro de dichos accesos.
122. Cuando sea necesario el acceso de otro tercero contar con la autorización expresa del administrador de los servicios y servidores.
123. Registrar quienes poseen las llaves o mecanismos de acceso a las instalaciones.
124. Informar a los guardas de seguridad a la salida y entrada de las instalaciones para que procedan a la activación de las alarmas y sistemas de seguridad instalados.

Control y normas en las instalaciones

125. Mantener en orden todo el material que se encuentre en las instalaciones.
126. Tener un inventario de todo lo que reposa en las instalaciones.
127. Mantener revisiones periódicas de los lugares, para detectar posibles inconvenientes, como fallas del suministro de energía, posibles humedades o exposición a condiciones adversas.
128. Mantener especial cuidado con la utilización de elementos inflamables o corrosivos que puedan deteriorar las mismas.
129. Mantener en óptimas condiciones los equipos de protección como extinguidores o elementos para actuar en situaciones imprevistas.
130. Realizar revisiones periódicas para detectar posibles alteraciones en las puertas y elementos de seguridad que se tienen.
131. Cuando se detectan fallos en los elementos de seguridad debe ser informado al personal encargado de este fin.
132. En las instalaciones se deben programar jornadas de aseo, para limpiar y verificar el estado de las mismas.
133. En las instalaciones no se deben realizar actividades diferentes a las del área, se debe evitar ingresar alimentos o bebidas, ya que esto atrae roedores o insectos que pueden generar daños.
134. Todos los administradores deben contar con acceso en cualquier horario, en caso

de que se presenten inconvenientes.

Centro de Datos IPET

135. El acceso está restringido únicamente a personal autorizado.
136. No se pueden realizar actividades diferentes a aquellas de administración de los equipos.
137. No se puede consumir bebidas ni alimentos.
138. Cuando se realice aseo en las instalaciones se debe realizar en compañía del administrador de los servicios o uno de los monitores.
139. Se debe mantener el registro de las personas que han ingresado, consignando la hora de ingreso, hora de salida y una descripción breve de la actividad que va a realizar.

Sala de administración de sistemas

Son las instalaciones donde se encuentran alojadas las estaciones de trabajo.

140. El acceso a las instalaciones se encuentra restringido a personal autorizado a la red de datos.
141. Las estaciones de trabajo de dicho lugar sólo pueden ser accedidas por los administradores.
142. Los administradores deben garantizar y cuidar que sus puestos de trabajo queden totalmente deshabilitados cuando ellos no se encuentran presentes.
143. Se debe mantener un registro de las personas que ingresan, la hora de ingreso y la hora de salida.

4.1.4 Equipamiento auxiliar

Corresponde a todos los equipos que contribuyen al correcto funcionamiento de los servidores.

Acceso

144. El acceso se debe restringir al personal del área encargada.

Mantenimiento

145. Establecer jornadas trimestrales de mantenimiento o por lo periodos que se consideren adecuados.
146. Se debe contar con una planta de suministro de energía que permita mantener la continuidad de los servicios cuando falta el suministro de energía eléctrica.
147. Se debe realizar mantenimiento preventivo a la planta en periodos definidos por parte de las personas encargadas.
148. La planta se debe encontrar en un lugar seguro donde sólo pueda acceder el personal autorizado.
149. En caso de fallas el administrador y los monitores del Centro de Datos deben tener los conocimientos mínimos que permita poner en funcionamiento la planta para suplir la falta de energía.
150. La planta debe cumplir con los lineamientos básicos para cumplir y suplir las necesidades básicas de los servidores, así mismo debe cumplir con las normas técnicas necesarias para cubrir el funcionamiento de los equipos que se encuentran alojados.
151. Se debe revisar periódicamente la planta para determinar que cuenta con el combustible y aceite requerido.
152. Se debe contar con un cronograma de mantenimiento para programar la salida de funcionamiento de los servidores.
153. Cuando la planta falla se debe informar el incidente al personal encargado de administración de realizar el mantenimiento de esta.

Sistema de refrigeración

154. Se debe contar con un sistema de refrigeración que permita mantener una temperatura óptima de trabajo en los equipos de red para evitar así posibles daños que se reflejen en un bajo rendimiento.

155. Se debe realizar mantenimiento preventivo del sistema de refrigeración por la empresa encargada para tal fin.
156. El administrador y los monitores deben contar con el conocimiento básico del funcionamiento del sistema, para cuando ocurren situaciones imprevistas puedan ser cubiertas.
157. Solo las personas encargadas de la administración de dicho sistema pueden realizar mantenimiento correctivo al mismo.
158. El mantenimiento correctivo de dicho sistema se debe programar con anticipación con el administrador de los servicios.
159. Este sistema no puede dejar de funcionar por un lapso de tiempo prolongado, ya se pueden generar grandes inconvenientes y se puede causar enormes daños en los equipos que se encuentran alojados.
160. Es necesario que diariamente los encargados de la administración lleven a cabo visitas para comprobar el funcionamiento del sistema.
161. Se debe revisar periódicamente.
162. Se debe capacitar a los monitores sobre funcionamiento básico.
163. No se debe apagar al menos que sea necesario.
164. Se debe mantener su nivel de refrigeración en el nivel adecuado.

Sistema de potencia auxiliar

Esta conformado por los equipos que permiten tener una fuente de potencia auxiliar para soportar la falta de suministro de energía eléctrica.

165. Las UPS deben estar sometidas a control semanal para comprobar las cargas de la misma.
166. Se les debe realizar mantenimiento preventivo en un periodo de tiempo no superior a seis meses.
167. Solo el personal autorizado y capacitado puede realizar los cambios pertinentes en los equipos.
168. Los administradores deben realizar visitas periódicas para observar la carga de los sistemas de tal manera que se pueda contar con un respaldo cuando falta la energía.

169. Los monitores deben contar con una capacitación básica sobre su funcionamiento.
170. Se debe revisar periódicamente su correcto funcionamiento.
171. Se debe informar de las posibles fallas al personal encargado.
172. Mantener una bitácora de funcionamiento y rendimiento.

4.1.5 Redes de comunicaciones

Mantenimiento:

173. Realizar mantenimientos semestrales de las redes de comunicaciones.

Acceso:

174. Restringir el acceso al personal encargado de las redes, llevando un registro permanente de acceso.

LAN

Esta compuesta por la tecnología que permite intercomunicar los servidores y equipos de red con los que cuenta el Centro de Datos de la Universidad del Cauca. Los elementos de la infraestructura de red se encuentran ubicados en el IPET. Estos elementos están conformados por puntos de acceso, cable Utp, bandeja concentradora, armarios para paneles de fibra y soporte de equipos.

175. Los puntos de acceso que no se encuentran en funcionamiento deben ser deshabilitados por el administrador, de tal manera que no se encuentran activos.
176. Se debe mantener por escrito el diseño de la topología de red que actualmente se tiene en funcionamiento.
177. Cuando se realice una modificación o cambio a la topología de red debe ser notificado y registrado.
178. Se debe revisar periódicamente el estado de la red interna, es decir emplear herramientas para determinar su throughput[16] y rendimiento.

[16] Throughput: eficiencia de la red.

179. Se debe revisar con Netflow o la herramienta que se tenga disponible el tráfico que esta circulando en la red para determinar posibles fallas.
180. Se debe mantener un informe de estos datos discriminado por áreas y dependencias.
181. Si se encuentran anormalidades o caídas en el rendimiento informar al área encargada para realizar las adecuaciones necesarias.
182. Se deben realizar pruebas de transferencias de archivos y pruebas de accesibilidad para determinar inconvenientes.

WAN

Corresponde a la infraestructura de red que permite acceder a Internet, esta infraestructura de red pertenece a las empresas con las cuales se tiene contratado este acceso, como los son ETB y EMTEL.

183. Se debe mantener por escrito el diseño de la topología de red que actualmente se tiene para estos dos canales.
184. Cualquier cambio o reparación en la infraestructura o en los equipos de los canales de acceso a Internet, debe ser registrado y notificado.
185. El mantenimiento y gestión de los canales es realizado únicamente por las empresas prestadoras del servicio.
186. Estas empresas deben garantizar la prestación del servicio, en caso de realizar mantenimientos preventivos, la programación de estos mantenimientos debe ser avalada por el administrador de los servicios y debe ser realizada en periodos no laborales.
187. Se debe verificar la capacidad entregada por el proveedor con herramientas como Netflow, Mrtg o Netexplorer.
188. Se debe diariamente verificar la conectividad con las redes externas utilizando direcciones conocidas y no tan conocidas.
189. Se debe realizar pruebas desde redes externas hacia la Universidad del Cauca. Verificar conectividad con ping u otras formas.
190. Se deben realizar pruebas de rendimiento.
191. Se deben realizar pruebas en condiciones normales de navegación y de descarga

de archivos. Verificar si se realiza bloqueo a algún tipo de tráfico.

192. Cuando se presentan fallas se debe informar de forma inmediata a las empresas proveedoras del servicio.
193. Se debe mantener un historial con la información sobre todas las fallas que se presenten.

4.1.6 Personal

Tipos de usuarios.

194. Se deben determinar claramente los tipos de usuarios que interactúan con el Centro de Datos, desde el usuario administrador hasta el usuario externo al entorno educativo.
195. Identificar las terceras partes que se involucran con el Centro de Datos, como lo son los proveedores de los enlaces de Internet, los técnicos que atienden el aire acondicionado, las UPS, etc. Sacar una listado de los mismos donde se encuentre especificado su relación, nombres, y contacto.

Acceso

196. Establecer los accesos de acuerdo a cada tipo de usuario.
197. Cuando se contrata personal externo para labores de implementación o instalaciones de cualquier tipo, estos deben ser supervisados y monitoreados por el personal del Centro de Datos.

Privilegios

198. Definir claramente los privilegios por tipo de usuario.
199. Todo el personal del Centro de Datos debe tener muy claras sus funciones y responsabilidades.
200. Los privilegios especiales, tales como la posibilidad de modificar o borrar los archivos de otros usuarios, esta otorgada solo a los administradores y encargados de la seguridad de los sistemas.
201. Los administradores no deben utilizar cualquier tipo de medio o información a la cual

tienen acceso para propósitos que no estén previamente autorizados.

Establecimiento de contraseñas

202. Los administradores no deben guardar las contraseñas en una forma legible en archivos en disco y tampoco de forma escrita en papel.
203. Cuando se sospecha que una contraseña ha sido comprometida se debe cambiar inmediatamente. No utilizar contraseñas similares a las establecidas anteriormente.
204. La contraseña es de uso confidencial, no debe compartirse, el hacerlo expone a las consecuencias por las acciones que los otros hagan con esa contraseña.
205. Las contraseñas por defecto que traigan nuevos equipos como *Routers*, *Switchs*, etc., deben cambiarse inmediatamente se coloque en servicio al equipo.
206. Para prevenir ataques, en los casos que sea posible, debe limitarse a tres el número de consecutivos de intentos fallidos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida por un tiempo determinado después del cual puede volver a reintentar.
207. Proteger meticulosamente las contraseñas y evitar que sean vistas por otros de forma inadvertida.
208. Establecer contraseñas robustas que no tengan ningún tipo de relación con su entorno familiar, de trabajo y demás. Contraseñas de mínimo ocho caracteres, con datos de tipo numérico, alfanumérico y de tipo especial.

Utilización de los equipos

209. Los equipos deben ser solo utilizados para fines sujetos a la misión del área.
210. No permitir o facilitar el uso de los equipos a personal no autorizado.
211. No utilizar los recursos informáticos y de telecomunicaciones para actividades que no estén relacionadas con los fines de la institución.
212. Los equipos deben usarse solo en ambientes seguros.
213. Se deben proteger los equipos para disminuir cualquier riesgo de robo.
214. Se deben marcar los equipos para el control de inventario.

4.1.7 Políticas específicas

215. La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y debe ser debidamente aprobada.
216. Cuando se entrega a un usuario una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
217. Se prohíbe el uso de cuentas anónimas o de invitado en los equipos, los administradores deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
218. Los administradores no deben acceder a los equipos inicialmente como "root", sino primero empleando su propio ID[17] y luego mediante "set userid" para obtener el acceso como "root".
219. Se debe establecer que las cuentas de usuarios deben caducar después de cierto periodo de inactividad, el cual se establecerá de acuerdo a las características propias de los servicios por los cuales se ingresa a esa cuenta.
220. Si el sistema de control de acceso no está funcionando apropiadamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
221. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
222. Generación de un informe anual del estado de seguridad actual.
223. Realización de un análisis de riesgo anualmente.
224. Se deben revisar todas las políticas de seguridad anualmente, después de realizado el correspondiente análisis de riesgos. Y en los periodos que se haga necesario debido a cambios organizacionales o de cualquier tipo que lo ameriten.
225. El personal del Centro de Datos debe mantenerse actualizado en todo lo referente a fallos de seguridad, lo cual puede lograrse a través de suscripciones a boletines de seguridad.
226. Informar de forma inmediata al administrador de los servicios de cualquier tipo de eventualidad que comprometa la seguridad en alguno de sus aspectos.

[17] ID: identificador.

227. Se debe reportar inmediatamente cualquier tipo de robo, incidente o pérdida de información y de cualquier dispositivo.
228. Activar el protector de pantallas al ausentarse del puesto de trabajo y programar el equipo para que lo haga de manera automática después de 5 minutos de inactividad siendo necesario volver a validarse.
229. Ninguna clase de equipo, información o *software* puede ser llevada al exterior sin la previa autorización del administrador de los servicios.
230. La selección del personal a laborar en el centro de datos, debe realizarse siguiendo un procedimiento acorde a los estatus o reglamentos, de manera que se pueda garantizar en gran medida la calidad del nuevo personal.
231. Todo el personal que labora en el Centro de Datos debe conocer y acatar las políticas de seguridad establecidas.
232. Se deben contar con procesos disciplinarios para todo el personal del Centro de Datos en caso de que incurran o fallen en el cumplimiento de las políticas trayendo con ello graves consecuencias.
233. Al terminarse el vínculo de trabajo por parte del personal que labora en el Centro de Datos, estos deben devolver cualquier tipo de equipamiento que le haya sido asignado, incluyéndose en estas tarjetas de acceso e identificación, llaves y demás. Así como cualquier tipo de privilegio anterior que gozaba por su vinculación.
234. Todos los tipos de cambios que se realicen por el personal deben ser documentados y se deben tener a disposición de las personas encargadas de la administración cuando se requiera.
235. Cualquier proceso de auditoria al Centro de Datos, así como la utilización de herramientas para este fin debe ser cuidadosamente planeado.
236. Para responder rápidamente a los incidentes de seguridad se debe establecer un procedimiento en el cual se especifique los pasos a seguir (escalamiento del caso).

4.2 Políticas de seguridad para los usuarios del Centro de Datos

4.2.1 Políticas para la utilización de servicios

El uso del servicio de correo electrónico es para los estudiantes, profesores egresados y administrativos, estos cuentan actualmente con la posibilidad de tener acceso a una

cuenta de correo electrónico de la Universidad del Cauca. La cuenta de correo les permite mantener y administrar sus correos, cuentan con una capacidad lo suficientemente grande para prestar un buen servicio, esta capacidad se complementa con archivos y con espacio para subir información, los usuarios pueden recibir todo tipo de correo sin ninguna restricción, actualmente dependiendo de la fuente se tienen algunas clasificaciones, por ejemplo algunos correos son clasificados como *Spam* según su procedencia.

Políticas para el uso de correo electrónico

1. Debe ser usado con fines personales y educativos que no atenten contra el libre y normal desempeño de las actividades educativas.
2. No debe ser usado para enviar contenido no deseado que pueda clasificarse como Spam[18].
3. No debe ser usado para enviar información que atente contra la integridad personal del destinatario.
4. Cuenta con una capacidad y un límite de almacenamiento determinado, no se debe sobrepasar dicho límite, para lo cual se pueden establecer tiempos de gracia que después de ser superados se procederá a la eliminación de la información para restablecer la capacidad establecida como límite.
5. Es recomendable no intercambiar información que se considere crítica o confidencial, cuando se requiera realizar se deben emplear métodos seguros que permiten cifrar la información para poder llevar a cabo los procedimientos.
6. No se debería emplear como medio para recibir respuestas de entidades o medios publicitarios, esto con el fin de reducir el Spam que llega a la cuenta de los usuarios.
7. Los usuarios cuentan con una carpeta denominada posible Spam en la que encontraran los correos que han sido clasificados como tal, estos correos se mantienen en esta capeta por un tiempo aproximado de 15 días, en los cuales automáticamente son eliminados de los servidores, esta carpeta debe ser revisada periódicamente para evitar posibles pérdidas de información.

Recomendaciones. El no cumplimiento de estas políticas puede ocasionar pérdidas de información de los usuarios, incluso grandes traumatismos por lo tanto se han previsto

[18] Spam: clasificación que se le da la correo electrónico no deseado, contiene contenido que no ha sido solicitado por el usuario.

algunas amonestaciones esto con el fin de reducir su riesgo:

1. Amonestación escrita que le informe el usuario que esta incumpliendo determinada política establecida.
2. Suspensión de la cuenta de usuario para acceder al correo por un periodo de un semestre, si persiste la situación o es recurrente puede causar la cancelación del servicio por tiempo indefinido.

Políticas para el uso del servicio de navegación por Proxy

El acceso a Internet se realiza por medio de servidores Proxy, los cuales permiten a la comunidad educativa acceder a Internet de una manera rápida y eficiente, dicho servicio puede ser empleado por cualquier miembro del estamento educativo de manera anónima, el servicio como tal tiene configurada políticas de seguridad que generan restricciones de acceso a lugares o puertos específicos que pueden causar una vulnerabilidad.

8. No se puede emplear el servidor Proxy para correr aplicaciones que son catalogadas como p2p.
9. No se puede emplear el servidor Proxy para pruebas de aplicaciones que pueden generar mal funcionamiento de la red.
10. No se puede emplear el acceso a Internet para realizar actividades que entorpecen el normal funcionamiento de redes externas.
11. No se puede emplear el acceso a Internet para realizar acciones que lesionan la integridad moral y física de las personas.
12. No se debería emplear el acceso a Internet para realizar descargas de contenido el cual no va a ser utilizado con fines educativos.
13. No se debería emplear para acceso a Internet de sitios que contienen información la cual no va a ser empleada con fines educativos.
14. Cuando se requiere el acceso a un sitio especifico el cual se encuentra bloqueado por el Proxy, se debe realizar una solicitud formal dirigida al administrador de los servicios indicando la necesidad de habilitar el acceso al puerto especifico, adjuntando en el mismo la justificación correspondiente.

Recomendaciones

3. Los usuarios que incumplan se verán sujetos a una amonestación escrita en la cual se les informe la causal de la misma, así mismo dichos usuarios deberán comprometerse a desistir de dichas actividades.
4. Si se persiste o es reiterativa la actividad, los usuarios pueden ser suspendidos temporalmente del acceso a Internet, o se les dará acceso restringido únicamente a los sitios necesarios para su labor educativa.

Políticas para el uso del servicio Ftp

El servidor FTP permite a los estudiantes de la comunidad universitaria publicar y mantener contenido de carácter institucional, de tal manera que cuenten con información disponible y de fácil acceso para el desarrollo de las actividades educativas que se tienen.

15. Para solicitar una cuenta en el servidor FTP se debe dirigir un oficio a él administrador de los servicios y se debe contar con los siguientes requisitos: ser docente o grupo de investigación reconocido y avalado por la Universidad del Cauca, sustentar en la carta la necesidad de utilización de una cuenta y especificar el tipo de información la cual va a ser alojada en este servidor, así como anexar los datos personales.
16. No se debe publicar contenido de tipo pornográfico o contenido que sea lesivo contra una institución o una persona.
17. No se debe publicar software que tenga algún tipo de restricción o del cual no se tenga la licencia respectiva para la distribución. El software que puede ser publicado debe estar regido bajo una licencia de libre distribución.
18. La cuenta creada para el usuario o grupo investigación tienen una capacidad máxima de almacenamiento, la cual debe ser tenida en cuenta y no se debe sobrepasar.
19. Los usuarios son totalmente responsables de la información que se mantiene en el FTP, cualquier pérdida de la misma es responsabilidad propia.

Recomendaciones

5. Si se incurre en alguna de las faltas el usuario recibirá una amonestación por escrito,

en la cual se manifestará la falta en la cual incurren y la necesidad de desistir del uso de la misma.

6. Los usuarios que no cumplan con dichas normas pueden ocasionar que la cuenta sea cancelada temporal o definitivamente según sea el caso de su incidencia.
7. Los usuarios son totalmente responsables de la información que publiquen, si la información atenta contra normas legales vigentes dicho usuario será responsable por las consecuencias que esto acarrea.

Políticas para el servicio hosting y de base de datos

Actualmente se puede solicitar un espacio Web en el servidor institucional, donde se puede mantener alojado un sitio y la información referente al mismo. Un espacio o hosting en los servidores, se asigna a una dependencia, facultad o departamento que haga parte de la Universidad y adicionalmente a los grupos de investigación que cuenten con el aval de un docente. Los estudiantes, docentes y administrativos también gozan de un espacio web personal desde el momento de creación de su cuenta de correo electrónico.

20. Para acceder a un sitio Web se debe dirigir un oficio en cual se consigne: la importancia y la necesidad de contar con un espacio Web, el contenido que será publicado, el responsable de administrar y mantener el contenido, el tipo de aplicación que se empleará para administrar y mantener la información, asimismo indicar si requiere la utilización de bases de datos.
21. La forma como se creará el nombre del sitio y la URL o dirección electrónica queda estandarizada y definida por www.unicauca.edu.co/nombre_del sitio.
22. El espacio Web personal de los estudiantes, docentes y administrativos queda estandarizado y definido por www.unicauca.edu.co/~nombredeusuario.
23. El contenido publicado en el sitio debe ser referente a la dependencia que lo solicita y debe mantener el carácter institucional.
24. No se puede tener contenido de tipo comercial o contenido que atente contra la dignidad de una institución o persona.
25. Las aplicaciones que se emplean para administrar y mantener este contenido deben ser lo suficientemente robustas, para que no generen una brecha de seguridad.
26. El código empleado para generar las aplicaciones debe estar lo suficientemente

filtrado de tal manera que no se generen problemas de seguridad debido a inconsistencias en el código.

27. Se debe tener mucho cuidado con aplicaciones que permiten crear foros o comentarios que quedan publicados en el sitio Web, es responsabilidad del administrador velar porque la información sea actualizada y verificada constantemente.

Recomendaciones

8. Si por una mala administración del sitio se presenta fallas en seguridad el administrador de los sitios es responsable por la información y por los problemas que se puedan generar debido a esto.
9. Si la información contenida en estos sitios no cumple con un contenido institucional o no se enmarca dentro de los procesos institucionales o es empleada con fines comerciales u otros que puedan atentar contra la dignidad de la persona o institución esta información será inmediatamente removida del servidor y el administrador será informado y amonestado por escrito por los percances ocasionados.
10. Cuando se presentan situaciones de riesgo en la cual el administrador del sitio es el responsable debido a una mala administración, el sitio Web puede ser cancelado temporal o definitivamente dependiendo de las consecuencias que una mala administración haya traído.

Servicio Web

El servicio Web es uno de de los servicios más importantes, ya que este servicio mantiene y aloja el portal institucional y muchas de las aplicaciones que se emplean para administrar gestionar y mantener muchas áreas administrativas y educativas con las que se cuenta.

28. El contenido del portal debe ser netamente institucional.
29. La responsabilidad del portal Web institucional recae directamente en la Red de Datos y sus diferentes dependencias: el contenido es responsabilidad del editor Web quien cuenta con el apoyo de un equipo de comunicadores; el desarrollo de aplicaciones es

responsabilidad del área de desarrollo Web; el diseño del portal esta a cargo del área de diseño gráfico.

30. La información que se publica en el sitio Web debe ser estudiada y referenciada de tal manera que se tenga certeza de la fuente y de la información que se está colocando.
31. El portal institucional es la cara visible de la Universidad del Cauca, por tal motivo es de suma importancia que este siempre presente.

Recomendaciones

11. Si un usuario atenta contra la integridad del portal institucional, este abuso debe ser reportado a las directivas quiénes tomarán las acciones pertinentes para su sanción dependiendo del impacto y los daños causados.

Servicio de DHCP

El servicio de DHCP consiste en la asignación de direcciones dinámicas a los equipos de la intranet universitaria, que necesitan conexión con la red interna e Internet.

32. Todos los usuarios tienen acceso y están habilitados para hacer uso del servicio de DHCP.
33. Los usuarios que hacen uso del servicio de DHCP no pueden emplear aplicaciones que entorpezcan el funcionamiento del servicio.
34. Para la navegación los usuarios cuentan con acceso a través de Proxy por tal motivo las aplicaciones p2p para descarga información no pueden ser empleadas.

Recomendaciones

12. Los equipos que utilizan aplicaciones no permitidas serán amonestados por escrito, si esa situación persisten dichos usuarios con su equipo serán bloqueados para acceso futuro, de esta manera en una próxima situación deberán dirigirse las instalaciones para que se les pueda otorgar una dirección interna para acceder a Internet.

Servicio RAS

La comunidad educativa de la Universidad del Cauca actualmente cuenta con la posibilidad de hacer uso del servicio de acceso remoto, y por lo tanto pueden solicitar la activación del servicio después de cancelar el pago estipulado, para esto se debe solicitar la creación de una cuenta de correo electrónico.

35. Los datos suministrados para el acceso remoto son él nombre de usuario (login) y la contraseña, que es la misma que se emplea para acceder al correo electrónico de la Universidad del Cauca.
36. El usuario deben contar con un buen sistema antivirus que evite que su computador se vea afectado con virus o aplicaciones que puedan perjudicar el normal desempeño de la red.
37. El acceso se debe realizar de una manera controlada y responsable de tal manera que no afecte las labores y las funciones de los servicios.

Recomendaciones:

13. Quienes incurran en faltas contra estas políticas serán sujetos a sanciones escritas, el continuar y persistir con estas actividades puede ocasionar la interrupción del servicio.

Asignación de direcciones públicas y NAT

Para solicitar acceso a Internet con direcciones publicas, se debe dirigir un oficio que relacione datos como nombre del solicitante, cargo del solicitante, justificación del uso de dicha dirección y la aplicación que va a emplear, así como los datos del equipo en la cual esta dirección será asignada. Es de recordar que sólo los docentes y grupos de investigación que justifiquen la necesidad de uso, tendrán asignada una dirección, este mismo procedimiento se emplea para el acceso a través de NAT global.

38. Quedan prohibidas las aplicaciones P2P, ya que por sus características son un riesgo potencial para la red.
39. Se debe contar con un buen antivirus que disminuya la posibilidad de que los equipos

se encuentren afectado por un virus.

40. La descarga de información debe ser controlada, esta información debería tener un carácter educativo.
41. Se debe contar con las suficientes medidas de seguridad que evite que el equipo sea accedido indebidamente por un usuario externo.
42. Las aplicaciones P2P o aplicaciones empleadas para hacer un mayor uso del ancho de banda deben usarse en los horarios permitidos y especificados por el área de servicios y servidores de Internet.

Recomendaciones

14. Los usuarios que incurren en amonestaciones y en uso indebido del acceso a Internet pueden verse sujetos a sanciones escritas, o el bloqueo de la dirección temporalmente cuando se usan aplicaciones no permitidas en días laborales.
15. Cancelación definitiva de la dirección que tiene asignada la persona, cuando incurren en esta actividad en situaciones reiterativas.

Políticas para la utilización de aplicaciones

43. Aplicaciones p2p: están totalmente prohibidas en horarios laborales, el uso de las mismas se debe justificar bajo un ambiente netamente educativo, el uso esta permitido en horarios no laborales en las cuales se tenga permitido su uso, la responsabilidad por el uso de estas aplicaciones recae sobre los usuarios que hacen uso de las mimas, por lo tanto ellos son los directos responsables de las incidencias y consecuencias que pueda traer su uso, tanto para el usuario como para la red. En caso de incurrir en una falta contra esta política, el administrador de los servicios esta en la facultad de eliminar las conexiones presentes y de restringir o bloquear la dirección IP de la máquina que esta generando tal cantidad de trafico. En caso de encontrarse de manera repetitiva el administrador esta en la facultad de cancelar el uso de esta dirección, de tal manera que quede restringido de manera permanente.
44. Para el uso de aplicaciones punto a punto que requieren tener buenas características de conexión y requieren de direcciones públicas o de NAT, se debe especificar la necesidad de la utilización de este tipo de aplicaciones y se debe sustentar la

necesidad en el entorno académico de tal manera que los administradores puedan realizar la gestión necesaria para llevar a cabo este proceso. Se debe adjuntar en la información el nombre de la persona el tipo de aplicación a emplear y el tiempo de uso de esta aplicación. Los puertos necesarios para emplear la aplicación, el destino de la conexión.

45. Aplicaciones de videoconferencia que requieren gran uso del canal. Para este tipo de aplicaciones se cuenta con equipos y con un direccionamiento especial el cual se debe asignar a estos equipos, de tal manera que para este tipo de eventos se pueda garantizar una calidad adecuada.

4.2.2 Información

Información almacenada en bases de datos

Esta información comprende todo lo referente a la información almacenada por los usuarios y las aplicaciones que tienen una cuenta y están posibilitadas para depositar información en dichos espacios.

46. Los usuarios deben realizar copias de seguridad de la información almacenada en sus cuentas usuario, por parte de los usuarios administradores de las aplicaciones en su cuenta personal.
47. Esta información sólo puede ser accedido por el usuario propietario de la información o la aplicación que hace uso de métodos para almacenar información.
48. Las cuentas para almacenar esta información cuentan con una capacidad máxima de almacenamiento.
49. Los usuarios son responsables de la información que se mantenga en estos sitios.
50. La información almacenada en la base de datos debe ser de carácter institucional y no puede contener material que atente contra la dignidad de una persona o institución asimismo el contenido de esta información no puede contener carácter comercial o pornográfico.
51. Los usuarios y administradores de la base de datos asignada deben garantizar que las aplicaciones que están utilizando no interrumpe o no genera inconvenientes que afecten el normal desempeño y funcionamiento del sistema, así mismo deben garantizar que el código y las aplicaciones no generan brechas de seguridad que

pueden afectar la información almacenada.

Recomendaciones

16. Las personas que incurren en circunstancias que afecten el desempeño serán notificados por escrito del inconveniente que están causando.
17. Si se presenta algún inconveniente debido a problemas en el código o aplicaciones con las cuales se almacena información en la base de datos, los administradores y propietario de dicha aplicación deben dar una solución pronta para evitar inconvenientes, si no se cuentan con un mecanismo inmediato para dar solución, el sitio o acceso a este espacio en la base de datos queda temporalmente cancelado.
18. Si el administrador de dicho espacio incurren en descuidos o faltas repetitivas que afecten el funcionamiento del sistema o la información que aquí reside, esta cuenta puede ser cancelada definitivamente.
19. Las personas que modifiquen o extraigan información de la base de datos que no corresponde a la información que ellos puede modificar serán reportados ante las autoridades competentes quienes tomarán las medidas respectivas.

Información almacenada en los espacios Web del servidor institucional

Corresponde a la información introducida por los usuarios que tienen una cuenta en el servidor institucional, los usuarios tienen autonomía de generar sus propios portales empleando aplicaciones como Mambo, Php, Java Script o HTML. Esta Información es administrada totalmente por los usuarios propietarios.

52. El contenido de la información debe ser de carácter institucional no puede tener contenido pornográfico o contenido lesivo contra la integridad de una institución o una persona.
53. Dicha información sólo puede ser accedida para ser modificada o eliminada por los usuarios propietarios de la misma.
54. Los usuarios administradores deben garantizar que dicho información será administrada de la mejor manera, es decir deben garantizar los mecanismos de seguridad pertinentes que evitarán que dicha información sea dañada o que genere

brechas de seguridad que afecten el funcionamiento del servicio Web.

55. Las aplicaciones que permiten almacenar y mantener la información en el espacio reservado deben garantizar la integridad de la misma, así mismo deben garantizar su fiabilidad y desempeño optimo, no pueden estar en fase de pruebas.
56. Se debe realizar copias de respaldo periódicas de la información contenida en dicho servidor, de tal manera que se puedan realizar recuperación de la información cuando ocurren incidentes no previstos.

Recomendaciones

20. Las personas que incumplan recibirán una amonestación por escrito.
21. Las personas que eliminen y que cambien información que no les corresponde sin autorización previa serán reportados ante las autoridades competentes.
22. La información almacenada en el espacio reservado para cada usuario que no cumpla con los requerimientos previstos puede ser bloqueada o incluso eliminada del servidor por los administradores de los servicios.

Información personal de los usuarios

Es información referente a cada usuario, que cuenta con una cuenta de correo electrónico y con un espacio para tener su página personal. Esta información sólo puede ser accedida por el mismo usuario propietario de la información.

57. El usuario debe garantizar y velar por el contenido de la información.
58. En el espacio personal de cada usuario la información contenida debe abstenerse de contener contenido lesivo contra una institución o persona, o contenido que atente contra la integridad, asimismo evitar tener contenido de tipo pornográfico.
59. La información de los usuarios cuenta con un determinado limite de almacenamiento, cuando se sobrepasa dicho límite el usuario queda imposibilitado para incrementar la capacidad de la información que tiene almacenada en el servidor.
60. En casos especiales a los usuarios se les puede incrementar la capacidad de almacenamiento que se tiene, para esto requiere de una justificación y una aprobación de carácter institucional.

61. Los usuarios deben evitar tener aplicaciones que generen traumatismos o inconvenientes para el normal desempeño y funcionamiento de la red.

Recomendaciones

23. Los usuarios que incurren en acciones en contra del reglamento serán informados por escrito y por correo electrónico de los inconvenientes que están causando.
24. Cuando un usuario mantiene información con un contenido que no esta enmarcado dentro de lo permitido por el ente universitario, dicha información puede ser bloqueada temporal o definitivamente.

4.2.3 Personal

Establecimiento de contraseñas

62. Los usuarios no deben guardar su contraseña en una forma legible en archivos, discos de almacenamiento, ni en papel.
63. Cuando se sospecha que una contraseña ha sido comprometida se debe cambiar inmediatamente. No utilizar contraseñas similares a las establecidas anteriormente.
64. La contraseña es de uso personal, no debe compartirse, el hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
65. Proteger meticulosamente las contraseñas y evitar que sean vistas por otros de forma inadvertida.
66. Establecer contraseñas robustas que no tengan ningún tipo de relación con el propio usuario, su entorno familiar o de trabajo.

Políticas específicas

67. La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y debe ser debidamente aprobada.
68. Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
69. Se prohíbe el uso de cuentas anónimas o de invitado, los usuarios deben entrar al

sistema mediante cuentas que indiquen claramente su identidad.

70. Las cuentas de usuarios deben caducar después de cierto periodo de inactividad, el cual se establecerá de acuerdo a las características propias de los servicios por los cuales se ingresa a esa cuenta.
71. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la institución y serán sancionadas por los entes correspondientes.
72. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
73. Informar de forma inmediata al administrador de los servicios de cualquier tipo de eventualidad que comprometa la seguridad en alguno de sus aspectos.
74. Se debe reportar inmediatamente cualquier tipo de robo, incidente o pérdida de información y de cualquier dispositivo.
75. Todos los usuarios de los servidores y servicios deben informar de cualquier inconveniente de seguridad que presencien al personal del Centro de Datos.

5. Criterios y recomendaciones para la generación y diseño del plan de contingencia para el Centro de Datos de la Universidad del Cauca

5.1 Introducción

El continuo desarrollo de las tecnologías de información y la comunicación con todas las facilidades, ventajas y beneficios que brindan para un mejor desempeño de todas las organizaciones, han hecho que su expansión sea tal que ya no se concibe ningún tipo de organización que no haga uso de ellas, desde las más pequeñas empresas hasta las grandes multinacionales y en todos los campos del que hacer, las TIC empapan el trabajo diario. Justamente la capacidad para permitir la realización de muchos trabajos cotidianos y de otros que hasta hace unos años no eran concebibles, han convertido a las TIC en imprescindibles en el mundo de hoy, por lo cual es tan inminente la necesidad de su permanente disponibilidad y funcionamiento acorde con especificaciones establecidas, pero es precisamente esta disponibilidad la que no cuenta con una garantía permanente, ya que cuanto más distribuidos y accesados son los sistemas más vulnerabilidades pueden surgir.

Es por esto que los planes de contingencia se han convertido en requisitos de primer orden a la hora de iniciar cualquier proyecto de tecnología en el cual se quieran establecer garantías y no un simple plan que solo se tiene presente cuando ocurre lo imprevisto, o lo previsto si se hacen bien las cosas. Hasta hace unos años el plantear planes de contingencia parecía ser asunto solo de grandes corporaciones, pero que en los mejores casos solo se limitaba a aplicar ciertas metodologías para copias de respaldo, pero en la actualidad no solo la pérdida de información, sino una corta interrupción temporal del servicio puede ocasionar grandes perdidas e importantes daños que pueden ser irremediables para cualquier organización, la alta disponibilidad de las TIC ya no es un lujo de unos pocos en tiempos anteriores sino una necesidad actual de muchos. Ya no es suficiente con tener establecido un plan de copias de seguridad, ahora son muchos los factores que se deben tener en cuenta en los sistemas cada vez mas distribuidos y de los cuales depende en gran porcentaje el trabajo diario, lo que hace más compleja la elaboración de un plan de contingencia.

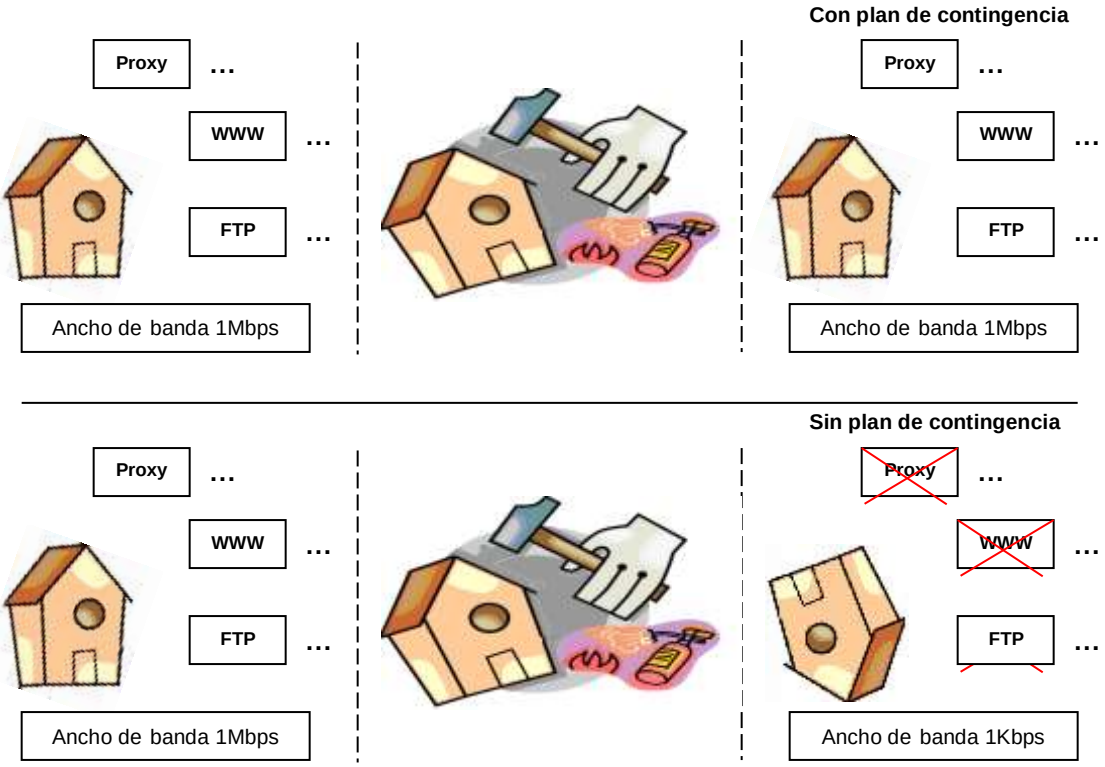


Figura 5. 1 Plan de contingencia para afrontar desastres

5.2 Definición

Un plan de contingencia se define como un conjunto de procedimientos y estrategias a seguir, tanto de carácter preventivo como correctivo, que permiten de manera rápida retornar a una situación que brinde una estabilidad lo suficientemente adecuada para que la organización pueda continuar con el desarrollo de todas sus funciones, en un nivel aceptable después de haberse presentado cualquier tipo de incidente no previsto, tanto interno como ajeno a la organización que haya provocado la interrupción o cese de cualquiera de sus funciones. [36]

Estos planes son diferentes de los de continuidad, en un plan de continuidad no hay interrupción del servicio y su costo es mucho mas elevado que el de un plan de contingencia, pero se debe tener claro que un plan de contingencia no es excluyente del de continuidad, mejor se considera que hace parte de este. [38] [40]

El plan de contingencia se refleja en un documento que especifica todas las acciones a seguir antes, durante y después de la contingencia, así como los responsables de cada

acción, se parte de la idea de que hay una parada de tiempo durante la cual se declara la emergencia y entran a operar la serie de procedimientos que permiten el restablecimiento de los servicios en el menor tiempo posible. Una vez solucionada la emergencia, se accionan otra serie de procedimientos que retornan las operaciones a un nivel de normalidad.

Un plan de contingencia se debe caracterizar por ser claro, preciso y conciso. Su orientación principal es el mantener la continuidad de las operaciones de la empresa, no solo la de sus sistemas de información. [37]

5.3 Importancia de establecer un plan de contingencia

Como ya se vio anteriormente a causa del desarrollo de casi todas las actividades de las organizaciones que están en constante contacto con las tecnologías de información, como lo son las empresas, grupos de investigación, instituciones de educación, etc, siendo para estas de gran importancia debido al tipo de información que manejan y la manera como deben gestionarla. Se hace obligatorio para estas organizaciones establecer planes de contingencia que permitan establecer altos estándares de calidad en la prestación de sus servicios. En toda empresa es parte integral de las responsabilidades del encargado de las TIC, garantizar la disponibilidad del sistema de información y de toda la infraestructura tecnológica que se requiera para que estos sistemas se puedan utilizar y acceder.

Es algo muy común que las instituciones educativas, no se preocupen por la creación de este tipo de planes, ya que erróneamente piensan que están exentas de eventos indeseables que pueden afectar las tecnologías utilizadas por el hecho de determinar que la probabilidad de que ocurra algún incidente es muy remota, o piensan que la información no debe ser tratada con los mecanismos que garantizen su seguridad, pueden ser incidentes como: desastres naturales o ataques terroristas, una torrentosa lluvia que puede causar daño a alguna conexión, una acción de vandalismo de un ladrón que puede parar las actividades de la empresa. [43]. Es un error pensar solo en los planes de contingencia por causa de grandes desastres naturales como huracanes, terremotos, tsunamis, inundaciones etc, que obviamente se deben considerar pero sin restarle importancia a otros eventos no naturales que pueden causar graves daños a la plataforma

tecnológica, como por ejemplo daños eléctricos, derrames de químicos, tóxicos o inadecuadas manipulaciones humanas por parte del personal de aseo por ejemplo.

El preparar un plan de contingencia no implica mostrar la ineficiencia en la gestión de las organizaciones, sino por el contrario contribuye a superar todas las situaciones que pueden provocar importantes pérdidas, no solo materiales sino también las causadas por el tiempo durante el cual no se presten los servicios.

Para entender la importancia que tiene el invertir en el desarrollo de planes de contingencia es suficiente con pensar en que sucedería si se perdieran todos los activos de información de una organización y no existiera posibilidad de recuperarlos, o que no se recuperen a tiempo o que al recuperarlos los datos no hubiesen conservado su integridad. [39]

5.4 Referente a Normatividad

La ISO ha planteado la norma ISO/IEC 27006[19], que esta orientado específicamente a la continuidad y recuperación, proporcionando guías para la recuperación de los servicios ante desastres, tanto propios como externos, lo cual reafirma el hecho de que los modelos de gestión están orientados a la seguridad de la información, establecido como un mecanismo para garantizar que los procesos que se basan en las tecnologías de información tengan un tratamiento optimo en beneficio de toda la organización.

Otro conjunto de recomendaciones internacionales que también abarcan el tema de gestión de la continuidad del negocio son la ISO 17799 y el CobiT de ISACA.

La norma ISO 17799, código de buenas prácticas de la gestión de la seguridad de la información, establece 10 dominios, de los cuales hay uno específicamente dedicado a la administración de la gestión de la continuidad del negocio, en el cual se destacan dos herramientas muy importantes: el análisis de impacto al negocio y el plan de recuperación de desastres.

[19] ISO/IEC 27006: Guidelines for Information and communications technology disaster recovery services.

En CobiT se tienen cuatro dominios, los cuales tienen a su vez procesos. Dentro de estos esta el proceso DS4[20], de aseguramiento de la continuidad de las operaciones,a su vez dentro de este proceso se tienen trece actividades que abarcan desde la creación del marco de referencia para la continuidad de las operaciones y la definición de una estrategia y filosofía de continuidad, hasta las indicaciones de contenido, implementación, prueba y distribución del mismo.

Los dos tiene diferentes enfoques, el enfoque de la norma ISO 17799 es de seguridad en los sistemas de información y el enfoque de CobiT es control de la información y de las tecnologías relacionadas, sin embargo los dos tienen aspectos similares en el caso de continuidad del negocio. Entre ellas esta la marcada necesidad de realizar un análisis de los procesos críticos para la operación del negocio y cuál debería ser la estrategia que la organización debería tomar en este sentido, estrategia basada en los objetivos de la organización y en el nivel de riesgo que esté dispuesta a afrontar. [41]

5.5 Beneficios de un plan de contingencia

El obtener una guía para implementar, operar y mantener un plan de contingencia, contribuye a mantener la disponibilidad de los servicios críticos, lo cual redunda en beneficios hacia los clientes, empleados y demás vinculados con la empresa, ya que logra que el impacto sea mínimo al exterior de la compañía. El principal beneficio que trae un plan de contingencia es garantizar el restablecimiento de los servicios que estén desmejorados por la falla en un periodo de entre doce y setenta y dos horas.

La existencia de planes de contingencia es una clara señal de los niveles alcanzados en materia tanto de competitividad, como de eficiencia administrativa en las organizaciones. Además se cumple con una exigencia que debe realizar cualquier tipo de auditoría interna en las empresas, para resguardar el patrimonio y continuidad del ente auditado, participando y monitoreando la existencia y puesta en ejecución de estos planes. [40]

[20] DS4: Proceso de aseguramiento de continuidad de las operaciones.

5.6 Criterios para la elaboración del plan de contingencia

La utilización de las TIC en los entornos universitarios es cada vez mayor, su uso es más generalizado y las instituciones se preocupan cada vez más por incorporarlas como herramienta fundamental en todos los procesos de enseñanza, aprendizaje, investigación, apoyo a la parte administrativa y de dirección universitaria. Las TIC son indudablemente una herramienta de mejora continua en el proceso docente.

Hasta la fecha su implantación ha logrado un buen alcance, pero se hace necesario que siga evolucionando y fortaleciéndose como pieza clave para aumentar la eficiencia en todas las instituciones de educación superior e ir modernizando la prestación de sus servicios y como elemento dinamizador de la sociedad de la información. Por lo anterior se debe incrementar la informatización de los servicios universitarios, lo que implica a su vez ir mejorando y estableciendo sistemas de seguridad como lo son los planes de contingencia. [50]

En la Universidad del Cauca, se deben tener en cuenta los siguientes criterios para establecer un plan de contingencia:

[1] Definir el planteamiento del plan de acuerdo a la actividad que produzca la contingencia, es decir si se quiere establecer un plan para afrontar cambios en el personal, desastres informáticos, desastres naturales, daños de máquinas, paros laborales, atentados, en fin, cualquier situación para la cual se puede diseñar un plan. [45] Determinar el tamaño de la institución, tener en cuenta el análisis de riesgos, la calidad y complejidad de los controles y políticas diseñadas.

[2] Establecer el personal humano que debe implicarse en la elaboración del plan, así como de acuerdo a la contingencia todos los actores que se verán involucrados, tener en cuenta el conocimiento de temática, la disponibilidad y la experiencia en estos procesos.

[3] Establecer el alcance y la aplicabilidad del plan a desarrollar. En esta parte se debe tener muy presente el aspecto económico. Tener en cuenta los costos, el tiempo, la aplicabilidad, la necesidad de implementarlo, la disponibilidad de recursos físicos y humanos.

[4] En general la ocurrencia de un evento adverso puede dividirse en tres etapas o ciclos, mostrados en la figura 4.2, creada en *Paint*. En el antes se plantea lo referente a prevención, mitigación, preparativos y alerta; en él durante se da la respuesta y en el después la rehabilitación y recuperación. [54] [49]

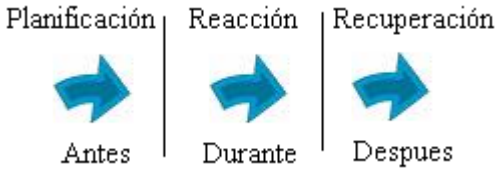


Figura 5. 2 Etapas de un plan de contingencia

[5] Adoptar una metodología de cinco etapas como la mostrada en la figura 4.3, para el diseño del plan.

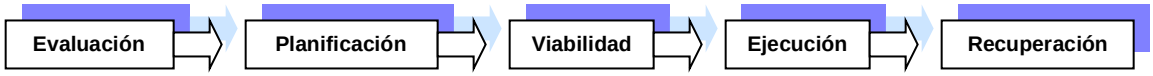


Figura 5. 3 Etapas sugeridas para el diseño de un plan de contingencia

[6] Dentro de la etapa de evaluación se deben considerar los siguientes puntos:

Tabla 5. 1 Criterios etapa de evaluación

Criterio	Descripción
• Constitución del grupo de desarrollo del trabajo.	Que debe ser coordinado por un responsable del plan y por los encargados de las áreas que se desean cubrir, así como estar continuamente supervisado y apoyado por la dirección.
• Identificación de las funciones críticas.	Identificar los elementos y funciones críticas para la organización en cualquier suceso indeseado y ordenarlas dentro de una jerarquía. Asignación de prioridades a las aplicaciones.
• Análisis de Riesgos.	Definición y documentación de los posibles escenarios de un incidente indeseado para cada función o elemento definido como crítico: se relacionan problemas con hardware, software, malos manejos de los sistemas de backups, incendios, cualquier eventualidad que pueda provocar pérdida masiva de información, problemas de energía y telecomunicaciones.
• Análisis del impacto del desastre en cada función crítica.	Realizar un análisis del impacto de cada problema sobre las funciones críticas de la organización, teniendo presentes criterios como el evitar pérdidas de vida, satisfacer las necesidades básicas, reanudar las operaciones lo antes posible, proteger el medio ambiente. Si es posible una cuantificación económica de cada problema esto ayudará a la selección de la solución alternativa.
• Definición de los niveles mínimos de servicio.	Establecer los niveles mínimos de servicio aceptables para cada problema que se pueda presentar, estos deben ser definidos con los responsables de las áreas que pueden ser afectadas.
• Identificación de las alternativas de solución.	Identificar las soluciones alternativas a cada uno de los problemas previstos.
• Evaluación de la relación	Con base en la alternativa establecida y el impacto económico

costo/beneficio de cada alternativa.	para cada problema, se determina la mejor solución con base en la relación coste/beneficio para cada proceso crítico y su tiempo de elaboración con el nivel mínimo de servicio establecido.

[7] Dentro de la etapa de planificación, tomar en cuenta los siguientes aspectos:

Tabla 5. 2 Criterios etapa de planificación

Criterio	Descripción
Documentación del plan de contingencia.	Es necesario documentar el plan, su contenido mínimo debe ser objetivo del plan, método de ejecución, tiempo de duración, costos estimados, recursos necesarios, evento a partir del cual se pone en marcha el plan y se designan personas encargadas de ejecutar el plan con sus correspondientes actividades. Asegurándose de que el plan es compatible con la estrategia presente y que es económicamente factible.
Validación del plan de contingencia.	El plan debe ser validado por los responsables de las áreas involucradas. Es importante tener presente las implicaciones de tipo jurídico que puedan derivarse de su ejecución.

[8] Dentro de la etapa de pruebas de viabilidad, tomar en cuenta los siguientes aspectos:

Tabla 5. 3 Criterios etapa de pruebas de viabilidad

Criterio	Descripción
Definir y documentar las pruebas del plan.	Se debe definir las pruebas del plan, con el personal y los recursos necesarios para su ejecución.
Obtener los recursos necesarios para las pruebas.	Recursos tanto físicos como de personal y demás que se hayan considerado necesarios.
Ejecución y documentación de las pruebas.	Lo cual sirve para evaluar el impacto real y detectar falencias del plan.
Actualizar el plan de acuerdo a los resultados obtenidos en las pruebas.	Gracias a los resultados de las pruebas del plan este se puede mejorar con todos los aspectos que se hayan presentado.

[9] En la etapa de ejecución, tener presente que el objetivo se centra en lograr la continuidad después de la contingencia y no en resolver las causas que la originaron, por ejemplo cuando falla un servicio principal como lo puede ser para una institución educativa el de correo electrónico, una solución para una recuperación pronta es instalarlo en un equipo de respaldo.

[10] Dentro de la etapa de recuperación, corregir los datos afectados de acuerdo a los procedimientos ya establecidos. Realizar un informe final con los resultados obtenidos de su ejecución. [45] [46] [56].

[11] Tener muy presente que en las situaciones para las cuales se establece los planes de contingencia, por lo general la prioridad es salvar la vida y después preocuparse por lo que haya sucedido con los servidores y equipos en general, en una situación de

emergencia la probabilidad de que se piense en lo que se debe hacer con respecto a las tecnologías es mínima, precisamente para eso se encarga el plan.

[12] Algo muy común para una recuperación es establecer una réplica de toda la infraestructura en otro sitio alejado del habitual donde tenga lugar el desastre, por lo anterior se habla de sitios calientes, templados, fríos y sitios espejo calientes. Los sitos calientes son aquellos cuya recuperación debe producirse en un máximo de 24 horas, los sitios templados tienen una tolerancia de uno a dos días de indisponibilidad, los sitios fríos son aquellos cuyo levantamiento puede tomar hasta tres días y los espejo calientes tienen una tolerancia de cero ante la recuperación, es decir funcionan en modo paralelo y entran en acción inmediatamente después de que el centro de datos principal ha sufrido el incidente. [66] Por ejemplo se puede pensar en el caso de la Universidad del Cauca en tener un centro de datos secundario alojado en un edificio diferente y en lo posible remoto al principal.

[13] Teniendo en cuenta todo lo anterior, se puede plasmar un documento que contemple los siguientes puntos:

• Contexto del plan, características del lugar de aplicación.
• Escenario de posible afectación por el evento, áreas, personal e infraestructura que pueden verse afectadas.
• Sistemas de alerta, activación y coordinación, números telefónicos de los responsables y la prioridad de llamada. Cadena de llamadas.
• Acciones operativas a implementar, listado de acciones
• Coordinación de las acciones, listado de personas responsables con la asignación de funciones. Quién hace qué, cómo, cuándo y con qué.
• Organización en el sitio, dibujo que ilustre la distribución de los elementos.
• Soporte logístico requerido, listado de implementos necesarios.
• Aspectos de seguridad integral, medidas de seguridad necesarias para la implementación del plan. [47] [53].

5.7 Recomendaciones

Algunas recomendaciones extras que pueden contribuir al éxito del plan de contingencia son las siguientes:

• Determinar las primeras señales de aviso de contingencia clave.
• Evaluar el contra impacto del plan, lo cual significa, estimar en qué medida capitalizará o cancelará su correspondiente contingencia.
• Establecer previsiones escalonadas.
• Analizar estadísticas.
• Involucrar a los actores externos (proveedores).
• Establecer un sistema ágil de comunicación con todos los involucrados, crear un directorio.
• Aclaración de dudas en la ejecución de pruebas del plan.
• Distribución y mantenimiento del plan.

• Envió de señales claras y seguras en caso de contingencias.

Otro aspecto importante es reconocer la importancia de no dejar solo en manos de los técnicos informáticos la responsabilidad de establecer el plan de contingencia, un ejemplo que nos sirve a comprender esto es el siguiente: "*en una competencia de fórmula 1 sería equivalente a pensar que el mecánico de coches es responsable de ganar una carrera, por supuesto que el papel de los mecánicos es clave para lograr el éxito y que pueden hacer una diferencia a favor o en contra, pero al final de cuentas, quien está al volante es el piloto, quien decide cuándo acelerar o cuándo rebasar, el piloto conoce su máquina y aunque delega su mantenimiento en los mecánicos, conoce lo suficiente para saber lo que puede obtener de su vehículo."* [44] Así mismo, la alta dirección es la responsable de entender la función de las tecnologías de información, de saber cómo puede esta función apoyar sus objetivos de negocio y de cómo pueden incluso plantear nuevos objetivos y servicios gracias a las tecnologías de información.

Algunas de las acciones que se pueden tomar para una recuperación ante desastres son las siguientes:

• Establecer un plan de verificación de las copias de seguridad.
• Escoger un software de copias de respaldo adecuado, teniendo en cuenta la importancia de su labor en el caso de ser requerido.
• Desplazar las copias de seguridad con cierta periodicidad a sitios externos a la organización, tener el adecuado cuidado de las copias en sitio.
• Mantener las máquinas aisladas, en entornos dedicados para su adecuado alojamiento.
• Cuidar de la ubicación de las máquinas, buscar que estén alejadas de redes de fontanería y desagües, que las tomas eléctricas sean seguras, garantizar el abastecimiento, que se tenga sistema contra incendios y que se cuente con sistemas de evacuación de emergencias, entre otros.
• No escatimar los posibles riesgos, cualquier daño imaginable tiene probabilidad de ocurrir e iniciando es mejor no descartar ninguno.
• Comunicar las acciones a tomar en todos los posibles incidentes, de nada sirve un plan que no sea conocido por los actores implicados.
• Es necesario invertir tiempo en la capacitación a todo el personal implicado, para que conozca bien las metodologías y tecnologías disponibles, por ejemplo conocer términos como BC/DR .
• Si es posible, ejecutar simulacros programados, lo que ayuda a obtener información sobre el proceso.
• Con la información recopilada elaborar una secuencia temporal de lo que se debe realizar en caso de un incidente. Información que será útil al ser analizada posteriormente para buscar maneras de optimizar el proceso.
• Después de haber identificado las posibles fuentes de incidentes con sus soluciones, se deben priorizar las partes del negocio para ordenarlas en importancia, ya que debe recuperarse lo que sea más vital o rentable para la organización. Por lo cual es necesario la vinculación directa y constante de la dirección de la organización, ya que es esta la que sabe que es lo más importante para el funcionamiento de su negocio, por lo cual debe ser ella quien establezca este tipo de prioridades. [41] [42]

6. Conclusiones y Recomendaciones

- El desarrollo del proyecto permitió profundizar a nivel educativo en un tema de gran importancia como lo es la seguridad de la información, en lo referente a la normatividad de la gestión de la seguridad de la información, la cual afecta directamente todos los procesos que esta envuelve, ya que apunta a introducir nuevos enfoques y paradigmas que mejoran los procesos y mecanismos a la fecha establecidos y empleados.
- Para el desarrollo de los lineamientos propuestos, con el fin de garantizar y generar los procedimientos de seguridad que mejor se acoplarán al Centro de Datos, se determinó que era muy importante para este proceso basarse en un estándar y una norma internacional, como la ISO 17799, debido a que actualmente Colombia no ha generado un estándar o una norma para la gestión de la seguridad de la información.
- Se optó por tomar como base los lineamientos dados en el RFC 2196 que se complementan de una manera adecuada con la norma ISO 17799 y permiten realizar los procesos de una manera ágil. Por tal motivo para la realización de los procesos de análisis de riesgos e implementación de controles y planes de contingencia se tomó como base las recomendaciones de la norma ISO 17799 y el RFC 2196 abriendo de esta manera los primeros procesos para que en un futuro el Centro de Datos de la Universidad del Cauca pueda iniciar un proceso de certificación en la norma ISO 27001.
- Se determinó que el Centro de Datos cuenta con algunas políticas de seguridad de facto que no se encuentran documentadas ni oficializadas, por lo tanto se consideran no existentes, por tal razón se tenian deficiencias en cuanto al manejo de la seguridad de la información.
- Se logró determinar que el Centro de Datos requería de un análisis de riesgos donde se determinarán los elementos más importantes para la prestación de los servicios a la comunidad, se identificarán los activos más relevantes, priorizarlos y definirlos claramente. Junto con la realización de una valoración de las amenazas que con mayor fuerza podrían afectar el funcionamiento.

- El empleo de herramientas y mecanismos de gestión de seguridad de la información ayudó a profundizar y obtener resultados que permitieron incrementar la formación y apropiación de esta temática de seguridad tanto a nivel administrativo del Centro de Datos como a nivel educativo.
- Se logró tener un presente teórico-práctico del análisis de aplicación de los lineamientos propuestos por los estándares de seguridad de la información, tomando como caso de uso práctico el Centro de Datos de la Universidad del Cauca al tener la aplicación de dichas normas en un ambiente real.
- Para el Centro Datos de la Universidad del Cauca realizar un estudio de análisis de riesgos, para implementar políticas y el plan de contingencia, permitió en gran medida definir y determinar el nivel actual de seguridad con el cual trabajan los elementos, equipos y personal que hacen parte de dicho centro, definiendo con este proceso los niveles reales de seguridad y la importancia de aplicar mecanismos de seguridad que permitan mantener unos niveles adecuados y aceptables para las características de funcionamiento del Centro de Datos.
- El desarrollo del proyecto permite crear conciencia en los administradores y usuarios de los servicios y servidores que hacen parte del Centro de Datos, de igual manera permitió definir la importancia de establecer niveles de seguridad adecuados que garanticen la continuidad en la prestación de los servicios basados en los estándares y lineamientos propuestos por la normas internacionales desarrolladas para este fin.
- Se mejoró el nivel de seguridad y la manera como se realizan los procesos y actividades para la gestión de la seguridad información, ya que se definieron los mecanismos y elementos como las políticas de seguridad para hacer frente situaciones de riesgo que en un momento dado pueden afectar el normal funcionamiento de los servicios y servidores.
- Manejar procesos de gestión de seguridad de la información en miras a que el Centro de Datos ingrese en un proceso de certificación, ayuda a posicionarlo como uno de los pioneros a nivel educativo en realizar dichos procesos, dejando las bases para que en un futuro se pueda optar por la certificación bajo el estándar ISO 27001.
- El establecimiento de un plan de contingencia para el Centro de Datos de la Universidad del Cauca, dada la importancia de las tecnologías de información en

su que hacer cotidiano, es de gran apoyo y fundamental para garantizar el restablecimiento de sus funciones vitales en un tiempo prudente, evitando así, en caso de presentarse desastres para los cuales fue diseñado, molestias y transtornos que la afecten gravemente en el desempeño de sus labores que hacen uso de los servicios prestados por el Centro de Datos, todo de acuerdo a un nivel de servicio mínimo establecido con anterioridad.

Recomendaciones para trabajos futuros

- El proceso de análisis y diseño de mecanismos de seguridad para solventar inconvenientes de seguridad realizados para el Centro de Datos, abre las puertas para que inicie procesos completos de análisis de seguridad e implementación de mecanismos con el fin de lograr en un futuro una posible certificación, con la utilización de herramientas para automatizar estos procesos, e incluso herramientas Web que permitan crear politicas de seguridad de manera práctica y automática. El diseño de un SGSI es un factor importante para un proceso de gestión y mejora continua de la seguridad de la información, por tal motivo es importante darle continuidad a un proyecto de este tipo que permita realizar este proceso en el Centro de Datos.
- Para llevar acabo este proceso de mejora continua en seguridad de la información, indudablemente es necesario continuar con procesos de gestión de seguridad que permitan llegar a automatizar los mismos mediante aplicaciones software que sean capaces de disminuir los tiempos empleados en estos procesos.
- En un futuro se puede profundizar en el alcance de las políticas de acuerdo a todos los aspectos que contemplan las normas internacionales, con miras a cumplir requisitos para una certificación.
- Es muy factible la creación de una aplicación web que facilite todo el proceso de certificación.

GLOSARIO

Activos: Es algo que tenga un valor para la organización, puede ser la información que maneja o administra, algún producto, el personal humano, los recursos físicos.

Política de seguridad: Conjunto de lineamientos con los cuales se logra mantener un orden y una sistematización. La información que se encuentra contenida en ellas describe o responde a muchos de los procesos o actividades de una organización, las políticas tienen consignadas las acciones que se deben y no se deben tomar.

Disponibilidad: Es la capacidad de que algo sea siempre este cuando se le requiere y que se pueda trabajar sobre este.

Confidencialidad: Propiedad que la información no esté disponible o sea revelada a personas que no están autorizadas para ver este tipo de información**.**

Integridad: Es la propiedad de proteger la exactitud y la plenitud de los activos.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Sin olvidar que otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y la no repudiación son contempladas y envueltas.

Evento de la seguridad de la información: Una ocurrencia del sistema, del servicio o de la red, indicando una posible brecha de información en cuanto a las políticas de seguridad se refiere, o puede ser un previo desconocimiento de una situación que puede ser relevante.

Incidente de la seguridad de la información: Evento inesperado que ha generado una brecha de seguridad o una respuesta a la preguntas de seguridad de tal manera que ha ocasionado, o puede ocasionar que la continuidad del negocio se vea afectada.

Certificación en seguridad de la información: Proceso que le permite a una organización ser reconocida por el cumplimiento de estándares establecidos internacionalmente, esta certificación garantiza que una empresa cuenta con los lineamientos que se han propuesto y especificado bajo las directrices de una organización internacionalmente aceptada y reconocida, como la ISO y la BSI.

Riesgo residual: Es el riesgo que queda después del tratamiento de riesgos.

Backup: copia de respaldo.

Plan de contingencia: Conjunto de procedimientos y estrategias a seguir, que permiten de manera rápida retornar a una situación que brinde una estabilidad adecuada para que la organización pueda continuar con el desarrollo de todas sus funciones, en un nivel aceptable después de haberse presentado cualquier tipo de incidente no previsto.

Intrusión Test: Test de intrusión, su objetivo es evaluar el estado de los sistemas y los mecanismos de protección frente a ataques o accesos no permitidos.

Hacking ético: Se denomina al evento de realizar pruebas e intentos de intrusión a determinados sitios con el fin de detectar los fallos y de esta manera poder corregirlos.

7. Bibliografía

[1] Políticas de seguridad, s-pdf/politicas_parte02.pdf. Documento disponible en: HTTP://mmc.igeofcu.unam.mx/LuCAS/Presentaciones/200203jornadassalamanca/slerena/politicas-pdf/politicas_parte02.pdf

[2] Políticas de seguridad, página Web disponible en: HTTP://es.tldp.org/Presentaciones/200203jornadassalamanca/slerena/politica.

[3] Seguridad de la información, HTTP://www.seguridaddelainformacion.com/seg_11.htm.

[4] Certificación en seguridad, certificacion_ISO27001.pdf, HTTP://www.nextel.es

[5] Proceso de certificación HTTP://www.sedic.es/c_procesocertificacion.htm HTTP://www.bsiamericas.com/Mex+Certificacion+CE/Que+es+la+certificacion+CE/El+proceso+de+certificacion+CE.xalter.

[6] Proceso de certificación ICONTEC, HTTP://www.icontec.org.co, Colombia HTTP://www.icontec.org.co/MuestraContenido.asp?ChannelId=632.

[7] Entidades certificadoras, HTTP://www.standardsglossary.com/

[8] Sitio oficial ISO disponible en: HTTP://www.iso.org.

[9] Sitio oficial BSI disponible en: HTTP://www.bsi.de.

[10] Beneficios de la certificación, página Web disponible en: HTTP://certification.bureauveritas.es/webapp/servlet/RequestHandler?mode=PT&pageID=31677&nextpage=siteFrameset.jsp

[11] Factores críticos del éxito, pdf Neosecure.pdf, documento disponible en: HTTP://www.itpro.cl/Seguridad/ISO27000/tabid/97/Default.aspx

[12] Sitio oficial Nextel, disponible en: HTTP://www.nextel.es

[13] Sitio oficial Applus+, disponible en: HTTP://www.appluscorp.com/esp/html/web.html

[14] Entidades certificadas, página Web disponible: HTTP://www.iso27001certificates.com/

[15] Sitio oficial español ISO 27000, HTTP://www.iso27000.es

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

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

[18] BS 7799, Gestión BS 7799.pdf. Documento disponible en: HTTP://www.bsi-global.com

[19] Norma ISO 13335, doc_otros_estandar_all.pdf. Documento disponible en: HTTP://iso27000.es/download/doc_otros_estandar_all.pdf

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

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

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

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

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

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

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

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

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

[29] ISO 15408, página Web disponible en: HTTP://www.iso15408.net/

[30] ITSEC, página Web disponible en: HTTP://www.itsec.gov.uk

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

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

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

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

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

[36] Planes de Contingencia II, HTTP://www.deltaasesores.com/prof/PRO045.html

[37] Planes de Contingencia I, HTTP://www.deltaasesores.com/prof/PRO044.html

[38] Continuidad y contingencia, HTTP://www.deltaasesores.com/prof/PRO189.html

[39] ,HTTP://www.deltaasesores.com/prof/PRO218.html

[40] Planes de continuidad/contingencia, HTTP://www.deltaasesores.com/serv/PDC.html

[41] Diez claves para una adecuada recuperación antes desastres,

HTTP://www.hispasec.com/unaaldia/2740.

[42] Seguridad en Unix: HTTP://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node1.html

[43] Planes de recuperación ante desastres, HTTP://www.hispasec.com/unaaldia/2540

[44] Apuntes de seguridad de la información, HTTP://www.HTTP://seguridad-de-la-informacion.blogspot.com/2006/04/seis-consejos-bsicos-para-recuperarse.htmlhispasec.com/unaaldia/2278.

[45] La auditoría interna y los planes de contingencia, HTTP://www.tuobra.unam.mx/publicadas/040710174457.html

[46] Articulo analizando un plan de contingencia, HTTP://www.virusprot.com/Art4.html

[47] Instituto nacional de defensa civil, planes de contingencia, HTTP://www.indeci.gob.pe/prev_desat/ley%2028551.htm

[48] Novatica, planes de contingencia y continuidad del negocio, HTTP://www.ati.es/novatica/2003/166/nv166sum.html

[49] Anexo VI Planes de contingencia.
HTTP://www2.unam.edu.ar/subprograma/metod_anex6.htm

[50] Informe sobre las TIC en las universidades de España, HTTP://www.aprendemas.com/Noticias/html/N2221_F25042007.HTML

[51] Planes de contingencia,.
HTTP://www.mnlibros.com.ar/DespLibro.asp?Libro=8479786477

[52] Planes de contingencia y continuidad del negocio, HTTP://www.seguridad-formacion.com/default.asp?pag=busqueda&id=995

[53] Plan de contingencia, S-3107 Formato Plan de Contingencia.pdf

[54] Planes de contingencia, Preparativos y Plan de Contingencia BsAs.pdf

[55] Planes de contingencia TIC, 166-3.pdf, Revista Novatica 166

[56] Recuperación de desastres. HTTP://www.disasterplan.com/

[57] Seguridad de TI, HTTP://web.mit.edu/ist/topics/security/

[58] Test de intrusion pagina disponible en :HTTP://www.isecauditors.com/es/test-intrusion.html

[59] Metodologia para realizar test de intrusion OSSTMM HTTP://www.isecom.org/

[60] Página web disponible en: HTTP://www.isecauditors.com/es/test-intrusion.html.

[61] Pruebas de intrusion pagina disponible en : HTTP://www.acis.org.co/archivosAcis/Inseguridad.doc.

[62] Página web disponible en: HTTP://www.penetration-testing.com/.

[63] Página web disponible en: www.cigital.com/papers/download/bsi6-pentest.pdf

[64] Página web disponible en: HTTP://www.vulnerabilityassessment.co.uk/ontr.htm

[65] Página web disponible en: HTTP://www.isecauditors.com/es/test-intrusion.html.