DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

EFRAIN ANDRES FAJARDO GUEVARA
MARÍA CONSTANZA TORRES BENAVIDES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2005

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁRTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

EFRAIN ANDRES FAJARDO GUEVARA
MARÍA CONSTANZA TORRES BENAVIDES

Trabajo para Optar al Titulo de Ingenieros de Sistemas

ASESOR: Ing. EDUARDO DELIO GÓMEZ LÓPEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2005

AGRADECIMIENTOS

Gracias a Dios, por la tranquilidad, la fortaleza y la claridad para guiarnos y encaminarnos por este camino.

A la Universidad de Nariño, gracias por abrir sus puertas y facilitarnos la información necesaria para la realización de este trabajo.

Al Director del Centro de Informática, Edwin Insuasty, por su valioso aporte para el desarrollo de este trabajo.

Henry y Freddy funcionarios del Centro de Informática, mil gracias por su incondicional disposición, colaboración y aportar su experiencia en el crecimiento de este trabajo.

A los funcionarios del las dependencias de OCARA, Almacén y Compras, Tesorería y Pagaduría, Contabilidad y Presupuesto, quienes con su disposición contribuyeron significativamente para el desarrollo de este proyecto.

Ing. Juan Carlos Castillo e Ing. Wagner Suero, gracias por apoyar esta iniciativa en el desarrollo de este proyecto y brindarnos sus conocimientos para el fortalecimiento de este trabajo.

A los jurados, Ingenieros, Henry Rodríguez y Francisco Solarte, quienes aportaron en nuestra formación profesional.

Ing. Delio, nuestro asesor, gracias por apoyar desde un principio esta iniciativa, por compartir su tiempo, sabiduría, experiencia y por darnos un mejor panorama de lo que debíamos hacer; sin su ayuda no sería posible haberlo terminado.

A todos quienes nos apoyaron durante todo este tiempo para desarrollar y finalizar este trabajo de grado, GRACIAS!!!, MIL GRACIAS!!!

DEDICATORIAS

Este nuevo paso es dedicado a las personas mas maravillosas del mundo, quienes me dieron la vida, me formaron y pusieron todo su empeño para llevarme hasta donde estoy, por eso este triunfo se los dedico a ustedes, Soco y Efrain, mis padres.

A mi esposa, Carolina, motor de mis emprendimientos, gracias a tu apoyo y tu amor, he logrado alcanzar mis objetivos, TPS.

A mi familia Ángela, Fernando, Anita, Álvaro, Guille, Pelu, Rocio, Pablo, Cata, Jaime, Cristina, Irmita y Daniel, por su apoyo y enseñanzas sobre los diferentes significados de la vida.

A mis amigos, que me han acompañado y ayudado en mis proyectos y en el desarrollo de este trabajo, Gelber y a todos los demás, que por el limitante de este papel no podré nombrar, pero que los llevo siempre en mi pensamiento.

Efrain

A Dios como Ser Supremo que me dio la vida, a mis padres, a mis hijos que me brindaron la fortaleza para hacer posible la realización de este sueño.

A mis padres, indudablemente, sin Ustedes no hubiera sido posible alcanzar esta meta propuesta, gracias por su comprensión y apoyo incondicional.

A mis hijos, David y Pipe, Ustedes han sido la luz de mi vida, la razón de vivir y luchar para salir adelante y así cumplir mis sueños y metas que siempre estarán en función de lograr lo mejor para Ustedes. MIS MUÑECOS LOS AMO CON TODO MI CORAZÓN.

A mi hermano, se que contigo cuento en todo momento, has sido un pilar de apoyo y ejemplo, gracias.

A todas las personas que han estado presentes en mi vida y de alguna manera han contribuido para el desarrollo y culminación de mi carrera, a todos, mil gracias.

María Constanza

CONTENIDO

	pág.
INTRODUCCIÓN	**15**
1. TEMA DEL PROYECTO	**17**
1.1 TITULO	17
1.2 MODALIDAD	17
1.3 ALCANCE Y DELIMITACIONES	17
2. DESCRIPCIÓN DEL PROBLEMA	**19**
2.1 PLANTEAMIENTO DEL PROBLEMA	19
2.2 FORMULACIÓN DEL PROBLEMA	19
2.3 SISTEMATIZACIÓN DEL PROBLEMA	19
3. OBJETIVOS	**21**
3.1 OBJETIVO GENERAL	21
3.2 OBJETIVO ESPECÍFICO	21
4. JUSTIFICACIÓN	**22**
5. ESTUDIO DE FACTIBILIDAD	**24**
5.1 TÉCNICO	24
5.2 ECONÓMICO	24
5.3 OPERATIVO	24
6. METODOLOGÍA	**25**
7. MARCO REFERENCIAL	**31**
7.1 MARCO LEGAL INSTITUCIONAL	31
7.2 MARCO TEÓRICO	31
8. PLAN GENERAL	**43**
9. INFORME GENERAL	**45**
10. CONCLUSIONES AUDITORÍA	**51**
11. POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.	**53**
11.1 INTRODUCCIÓN	53
11.2 CONTENIDO POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.	54
12. CONCLUSIONES	**126**
BIBLIOGRAFÍA	

LISTA DE ANEXOS

	pág.
Anexo A. Archivo Corriente	127
Anexo B. Archivo Permanente	398

RESUMEN

El presente trabajo , es el resultado de la investigación en seguridad informática realizada en el Centro de Informática de la Universidad de Nariño, aplicando una metodología de Auditoría de sistemas para determinar los riesgos, que permitieron identificar las debilidades que tiene esta dependencia en relación con la seguridad.

Enfocando los resultados de la investigación y convencidos que la manera de mejorar la seguridad de la información es a través del establecimiento de lineamientos claros y enfocados a los sectores principales, se desarrollaron unas políticas de seguridad orientadas al Centros de Informática de la Universidad de Nariño, que les permita reducir los riesgos frente a posibles ataques o problemas inesperados, reduciendo así las probabilidades de pérdida de confidencialidad, integridad y disponibilidad de la información. La seguridad es un proceso dinámico que día a día se debe ir redireccionando frente a los nuevos avances de tipo tecnológico y conocimientos cambiantes y evolutivos de las personas.

El trabajo plantea la seguridad desde el punto de vista físico y define los controles que se deben manejar, para reducir los posibles problemas como robos, accesos no autorizados, emergencias, mantenimiento, entre otros, a través de políticas organizadas en lo relacionado con la seguridad frente a la construcción de edificaciones, controles ambientales que deben tenerse en cuenta en las áreas donde se realiza procesamiento de datos, medidas para asumir posibles desastres, controles de accesos a las instalaciones, protección para los equipos de computo.

La seguridad a las instalaciones eléctricas es otro de los aspectos relacionados en el presente trabajo, con lo que se poduede identificar las medidas de seguridad que se deben aplicar en el manejo de redes eléctricas y sistemas de respaldo eléctrico, basándose en los estándares y normatividad existente para estas áreas.

Las redes de datos ha generado sin duda muchos de los avances de la informática moderna, generando dinamismo y optimización de recursos a las organizaciones por lo cual fue tema de estudio de nuestro trabajo, en donde se estudio las redes físicas de datos, los servicios lógicos que prestan las redes y lógicamente las prevenciones que se deben tener en cuenta al realizar la utilización de la red mundial y seguridades que se deben aplicar a los equipos servidores que prestan los servicios en Internet.

La seguridad lógica, se enfoca en los mecanismos que se deben contemplar en el uso de recursos informáticos, administración de sistemas y servicios, desarrollo de software, redes de datos y respaldos lógicos.
La seguridad en el personal, plantea los lineamientos a seguir en el control de usuarios, claves de acceso, acceso físico, seguridad en la utilización de recursos informáticos.

El trabajo plantea directrices que deben implementarse desde la parte directiva en la Universidad como políticas de cumplimiento obligatorio a las cuales se les debe realizar un seguimiento continúo y debe ir acompañado de planes de mejoramiento a la par con el avance tecnológico que planee y implemente la Universidad.

ABSTRACT

The following paper is the result of a research performed on computer security that took place at the computer center at Universidad de Nariño, applying a computer systems auditorship in order to determine the possible risks, that allowed us to identify this office's weaknesses in relation to security.

Considering the reseach results and being convinced that the best way to improve the information security is throughout the stablishment of clear lineaments focused to main sectors, some new security policies oriented to the computer center at Universidad de Nariño were developed. All this will help to reduce the risks of possible attacks and unexpected problems, reducing the possibility of loss of confidenciality, integrity and availability of information. Security as dinamic process should be directed towards the new technological advances and people's changing and evolving of knowledge day by day.

This paper outlines the security from a physical poing of view and defines the controls that must be used in order to reduce possible problems such as stealing, unauthorized accessing, emergencies and maintenance among others, through well planned policies related to building construction security and environmental control. Such controls must be carried out in areas were data processing, the creation of measurements to assume possible dissasters, premises access control, and computer equipment protection are been performed is created.

Electrical installation security is another aspect planned in this paper. Thus, it can be possible to identify the security meassurements that should be applied in the handling of electrical network and electrical backup systems based on the standar compliances that exist in these areas.

It is well known that data network have generated many of the modern computer advances, creating dynamism and improving the companies resources where the physical data network and the logic services provided by the network take place. For this reason it is important to say that a great number of precautions when using the internet and the security protocols must be taken into account and applied to the server equipment that provides the internet service.

Logic security is focused on the mechanisms that should be taken into consideration when using computer resources, computers and sevices management, software development, data network and logistic backup. Personnel security outlines the procedures to follow in the users control, access passwords, physical access and security resources.

The paper also suggests mandatory policies that must be stablished by the university director's board which would have a very close follow up procedure besides being accompanied by improvement plans along with technological advances implemented by the institutional directives.

INTRODUCCIÓN

La seguridad es un concepto amplio y complejo concebido dentro de todos los ámbitos que nos rodean, considerado desde la antigüedad, que ha evolucionado con el desarrollo de las culturas y organizaciones sociales.

Desde finales de la década de los ochenta, el tema de seguridad informática ha formado parte de las empresas, aunque muy poca gente, empresas e instituciones han tomado en serio el tema de la seguridad informática, mientras el desarrollo de nuevas tecnologías informáticas van creciendo exponencialmente, inherentes a ellas nuevas formas de atentar contra los sistemas de información, es así, como la existencia de políticas y procedimientos de seguridad, se convierten en una necesidad para dar solución a los problemas a los cuales se enfrentan las instituciones en lo que se refiere a la protección de la información y recursos informáticos frente a amenazas externas e internas, accidentales o intencionadas.

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican lo que esta permitido y lo que no, con el fin de aumentar el nivel de seguridad de los sistemas informáticos, indican que controles tomar para proteger un sistema y forman la base para la implantación efectiva de medidas de protección de los recursos informáticos, entonces, se pregunta ¿Qué se quiere proteger?, en un sistema informático se protegen tres elementos fundamentales, el software, el hardware y la información, siendo el último elemento quizás el mas importante de proteger, porque según afirman algunos autores es el mas amenazado y difícil de recuperar, y es que las medidas de seguridad son precisamente para garantizar la integridad, disponibilidad y confidencialidad de la información.

Y pensando en la importancia de la información en los procesos sistematizados de la Universidad de Nariño, este trabajo de Definición de Políticas de Seguridad Informática, pretende, establecer unos criterios para la protección de los recursos informáticos y de la información que maneja el Centro de Informática de la Universidad, así con estas directrices lo que se busca es orientar en el uso de las nuevas tecnologías de manera que estas se conviertan en una herramienta de aprovechamiento para la Institución y no se conviertan por su mal uso, en amenazas que puedan irrumpir en la prestación de sus servicios.

Para la definición de políticas, fue preciso utilizar como metodología una Auditoría a la seguridad de los sistemas de la Universidad, identificando los recursos y los activos que dispone, las vulnerabilidades en los procesos que realiza, los servicios que presta, reconocer las dependencias o personas a las cuales ofrece servicios

y los objetivos propuestos en el Centro de Informática en su función de procesamiento de la información.
Conociendo así los procesos de la Universidad y la disposición de recursos, el propósito de este trabajo, es definir políticas a los usuarios del sistema con las obligaciones que deben asumir respecto a la seguridad y dar las pautas para actuar ante posibles amenazas y problemas presentados, de manera que estas políticas de seguridad, estén al alcance de la Universidad y se implementen para así mejorar el nivel de seguridad, lo ideal es que se invierta en la seguridad y esto ofrezca un equilibrio dentro de la organización entre el riesgo y la seguridad. Cabe resaltar que no hay sistema ciento por ciento seguro lo que se hace es minimizar el riesgo.

Naturalmente, las políticas no son estáticas, en un medio tan cambiante las nuevas tecnologías informáticas y de comunicación traerán consigo, nuevas fallas y debilidades, las cuales deberán ser detectadas por las directivas de la Universidad y establecer un compromiso para actualizar las políticas según las nuevas circunstancias que enfrente la Institución.

La auditoría de sistemas con su objeto de evaluar el grado de protección que tiene una organización frente a posibles amenazas a las cuales esta expuesta, se convierte en parte fundamental para el diseño e implementación de políticas de Seguridad. No basta con diseñar buenas políticas, es necesario llevarlas a la práctica en forma correcta y garantizar que se adecuen a las condiciones de la institución.

1. TEMA DEL PROYECTO

1.1 TITULO

DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

1.2 MODALIDAD

El trabajo de grado que se presenta a continuación se enmarca dentro de la modalidad de Trabajo de Investigación.

1.3 ALCANCE Y DELIMITACIONES

La definición de políticas de seguridad pretende establecer unos lineamientos claros para el manejo adecuado de la infraestructura informática, y de los sistemas de información involucrados en el procesamiento de la Información Administrativa-Financiera y Académica, que maneja el Centro de Informática.

Las políticas de seguridad se definirán para el Centro de Informática de la Universidad de Nariño sede Torobajo, enmarcadas en los siguientes puntos de seguridad informática:

Seguridad Lógica:
Establecer bases de seguridad para el manejo de software en los niveles de Sistema Operativo, Software manejador de Base de Datos, Bases de Datos, Software Aplicativo, Software de Control de Acceso, Software Antivirus, Aplicaciones para la publicación de información en Internet, Software desarrollado a la medida y futuros desarrollos; para garantizar que la información y recursos de software que maneja el Centro de Informática sean siempre utilizados de forma correcta, autorizada y en actividades exclusivas del Centro de Informática, controlando acciones que puedan provocar su alteración, borrado o divulgación no autorizada de forma accidental o intencionada .

Seguridad en el Personal:
Establecer políticas de seguridad en aspectos relacionados con el acceso a la Información por parte de los usuarios, como también el acceso físico a las instalaciones, con el fin de reducir los riesgos ligados a posibles errores humanos.

Seguridad Física:

Establecer lineamientos de seguridad para las zonas que contengan recursos informáticos del Centro de Informática y sus entornos, en los aspectos relacionados con la ubicación, instalaciones físicas, acceso a las oficinas, elementos constructivos internos (puertas, ventanas, paredes, suelos.), buscando controlar riesgos potenciales de ataque, pérdida, robo o daño a los equipos y periféricos, ya sean estos accidentales, intencionados o bien causados por desastres naturales, que puedan ocasionar la interrupción, total o parcial, de sus actividades.

Seguridad de la Instalación Eléctrica:
Definir lineamientos de seguridad para instalaciones eléctricas en el Centro de Informática y sus entornos en lo relacionado a la red eléctrico y el suministro de energía. Los sistemas eléctricos son ambientes muy sensibles y pueden ocasionar fallas de energía produciendo pérdidas de información, de trabajo y equipos.

Seguridad de la Red de Datos y las Comunicaciones:
Establecer políticas enmarcadas en normas y estándares para instalación e implementación de Redes de datos física y la conexión a Internet con el fin de asegurar que la comunicación y los datos en la intranet se operen de una manera correcta y segura, en todos los puntos y medios de transmisión, garantizando una óptima gestión de la red, procedimientos para acceder a la Información y procedimientos para el intercambio de información.

2. DESCRIPCIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

El Centro de Informática de la Universidad de Nariño, no tiene establecido lineamientos de seguridad informática, que respalden los procesos de protección relacionados con los recursos informáticos, que están bajo su administración.

En los últimos años la Universidad de Nariño ha evolucionado en el campo de la tecnología informática y la sistematización de su información, sin embargo dentro de este avance no se ha contemplado un aspecto fundamental dentro de los procesos sistematizados que garantiza la integridad, confidencialidad y disponibilidad de la información, como lo es la seguridad informática.

Así mismo, ese amplio desarrollo de tecnologías trae inherente una serie de acciones y mecanismos delictivos y antisociales, que ponen en peligro la información, aprovechando las vulnerabilidades tanto a nivel físico como lógico que puede presentar la organización.

El Centro de Informática no exento a este tipo de conductas debería considerar dentro de su estructura funcional, un esquema de seguridad que especifique la normatividad que deben tener los elementos que interactúen con esta dependencia, reduciendo riesgos a problemas tales como la perdida de información y equipos, la suplantación de usuarios, el espionaje de información sensible o incluso el incumplimiento de la normativa vigente, estos riesgos traen consigo la necesidad de un esquema de seguridad que defina las características, estándares, políticas y procedimientos de los elementos que constituyen el Centro de Informática.

2.2 FORMULACIÓN DEL PROBLEMA

- ¿Existe un documento que determine la situación actual de la seguridad de sistemas del Centro de Informática de la Universidad de Nariño?

- ¿En la actualidad existe un esquema de seguridad, basado en políticas que definan mecanismos para garantizar la integridad, confidencialidad y disponibilidad de la información en el Centro de Informática?

2.3 SISTEMATIZACIÓN DEL PROBLEMA

- ¿Existen procedimientos bien definidos, que controlen el acceso de usuarios al sistema, operación, manipulación y vigilancia de los elementos del Centro de Informática?

- ¿Existen procedimientos que garanticen el respaldo de la información?

- ¿Existe documentación sobre el desarrollo y modificación de software?

- ¿Cumple el Centro de Informática, con las normas y estándares, para la ubicación y construcción de un centro de cómputo?

- ¿Se cuenta con una red eléctrica adecuada, que cumpla con los requerimientos eléctricos y normatividades, para el funcionamiento del Centro de Informática?

- ¿Se cuenta con estándares de cableado estructurado y dispositivos adecuados que permitan la comunicación y transmisión segura de la información?

3. OBJETIVOS

3.1 GENERAL

Definir políticas de seguridad informática claras, que orienten a los directivos del Centro de Informática de la Universidad de Nariño, a establecer un esquema de seguridad que garantice la confidencialidad, integridad y disponibilidad de la información, el software y el hardware, para lograr un mejor aprovechamiento de los recursos.

3.2 ESPECÍFICOS

- Realizar un análisis de la eficacia del sistema de seguridad del Centro de Informática, en los campos de software, personal, redes de datos, redes eléctricas, instalaciones físicas y control de acceso.

- Verificar la implantación de las normas y estándares en el esquema de seguridad actual del Centro de Informática.

- Identificar riesgos y vulnerabilidades que ponen en peligro la seguridad de la información y de los recursos, y analizar medidas que disminuyan la probabilidad que estos ocurran.

- Minimizar a través de políticas de seguridad riesgos que amenacen a los procesos del Centro de Informática.

- Establecer lineamientos para el manejo de los recursos informáticos con el fin de controlar riesgos potenciales de ataque, pérdida, robo o daño a los Sistemas de Información de la institución, accidentales o intencionados, que puedan ocasionar la interrupción, total o parcial, de las actividades de la Universidad.

4. JUSTIFICACIÓN

La seguridad informática es uno de los talones de Aquiles de los sistemas de información actuales, dados los nuevos adelantos en comunicaciones y tecnología, así como los avanzados conocimientos en computación de las personas (jóvenes y adultos) que demuestran sus aptitudes en técnicas de hacking y espionaje informático, entre otros, lo que ha generado una gran inquietud sobre como las instituciones están asegurando y previniendo los ataques a sus sistemas informáticos.

La seguridad informática pretende garantizar la confidencialidad, integridad y disponibilidad de la información, a través de un conjunto de recursos técnicos y lógicos con los cuales se logren estos objetivos, como el estudio a la seguridad con la cual se desarrolla una investigación y evaluación a los procesos sistematizados para indagar la fiabilidad, eficiencia y eficacia de un sistema. Así, generar una herramienta de soporte para la toma de decisiones y correctivos, que es en ultimas en lo que se convierte el informe de Auditoría , otro de los recursos son las políticas de seguridad que son manuales de referencia para el desarrollo adecuado de ciertos procesos con el fin de que estos se ejecuten de manera segura, además orientan el manejo de la información y sus entornos. Otro de los recursos con los que se cuenta para reforzar la seguridad informática son los planes de contingencia a través de los cuales se especifican las tareas y actividades puntuales que se desarrollaran frente a ciertos acontecimientos probables.

Dado que los sistemas de información y su manejo son tan diversos, se han establecido algunos estándares y normas que pretenden guiar y mejorar la seguridad de la información sirviendo como base para el desarrollo de planes, políticas y estudios específicos de las instituciones, es importante destacar que los planes y políticas deben ajustarse específicamente a los requerimientos, circunstancias y procedimientos de cada una de ellas.

Concientes que el conocimiento y el manejo de la información es el recurso más importante de toda institución y que es deber de las directivas gestionar e impulsar la adquisición del mismo, se pretende realizar la Auditoría a la seguridad informática del Centro de Informática con el fin de aportar una herramienta conceptual que permita a las directivas conocer el estado actual de esta dependencia y realizar los correspondientes correctivos y mejoras a la misma según unas políticas establecidas.

Existe la necesidad de elaborar políticas de seguridad que permitan establecer unos parámetros concretos y basados en hechos actuales, que sirvan como base

para el funcionamiento de esta dependencia en lo relacionado con la seguridad de la información tales como políticas de manejo de software, políticas para instalaciones físicas, red eléctrica, políticas para desarrollo de software, políticas para adquisición de software, manual de funciones, políticas para redes físicas y lógicas.

5. ESTUDIO DE FACTIBILIDAD

5.1 TÉCNICO

Para el desarrollo de este trabajo se utilizaron equipos de cómputo, cámaras fotográficas, grabadoras, filmadoras, multímetro digital y certificadores de red.

5.2 ECONÓMICO

Los recursos necesarios para el desarrollo de este trabajo de grado serán materiales de papelería y alquiler de dispositivos, gastos asumidos por los estudiantes.

5.3 OPERATIVO

Los recursos humanos con los que se cuenta, es el equipo de trabajo para el desarrollo de la Auditoría conformado por los estudiantes EFRAIN FAJARDO Y MARIA CONSTANZA TORRES, además se cuenta con el apoyo del Ingeniero especialista en Auditoría de sistemas DELIO GOMEZ, el Ingeniero Eléctrico WAGNER SUERO, el Ingeniero JUAN CARLOS CASTILLO, personal del Centro de Informática y de las dependencias de estudio.

La Auditoría de sistemas se desarrollará en el Centro de Informática de la Universidad de Nariño, logrando como resultado final el documento de Políticas de Seguridad del Centro de Informática y el informe de Auditoría , dirigido al Director del Centro de Informática y Comité de Sistemas.

6. METODOLOGÍA

La definición de Políticas de Seguridad se realiza en base a un proceso de investigación de vulnerabilidades y riesgos para lo cual se utiliza como herramienta la Auditoría de Seguridad de Sistemas del Centro de Informática, considerando esto, es necesario realizar la Auditoría correspondiente, obedeciendo a unos principios generales de Auditoría , utilizando técnicas de cuestionario, observación, confrontación, indagación y evidencias.

La metodología de investigación a utilizar en el proyecto es la siguiente:

- *Recopilación de Información:*

Se solicitó al Centro de Informática de la Universidad de Nariño, información en lo que se refiere a normas, políticas y procedimientos vigentes en la dependencia para el desarrollo de las actividades vinculadas al procesamiento de la información y su interacción con el entorno informático, también, se hizo petición, de documentación que señale los objetivos y funciones del Centro de Informática, la relación de software existente para los equipos de funcionamiento en esta dependencia y documentación relacionada con el desarrollo de aplicaciones.

A la oficina de Planeación de la Universidad de Nariño, se solicitó: Planos de instalaciones, planos de la red eléctrica, planos de la red de datos, Planta de Personal, Estructura Orgánica y Manuales de Procedimientos y Funciones; todo en relación con el Centro de Informática y las dependencias de estudio como son: OCARA, Almacén y Compras, Contabilidad y Presupuesto, Tesorería y Pagaduría, y la Oficina de Recursos Humanos.

Al Director del Aula de Informática se solicitó, la relación del software licenciado para la Universidad de Nariño, al igual que las fichas de mantenimiento para control de software instalado en los equipos del Centro de Informática y las dependencias concernientes para este trabajo.

Se hizo la petición al Comité de Sistemas de un documento que especifique sus funciones como ente orientador en los procesos informáticos de la Universidad, además, se solicitó el informe que relaciona la creación de la Unidad de Mantenimiento.

Se solicitó a la Oficina de Almacén y Compras el listado del inventario actualizado que contemple software y hardware existentes en el Centro de Informática.
La documentación que se señala anteriormente fue entregada de acuerdo con la existencia y disponibilidad de la misma.

- *Identificación y selección de los ambientes a auditar:*

Los ambientes de estudio para este trabajo se escogieron de acuerdo a la relación que tengan con el Centro de Informática para el desarrollo de sus actividades, de manera que la ausencia o falla de estos elementos no alteren el cumplimiento de las mismas.

Como ambientes se señala: El entorno físico de las instalaciones del Centro de Informática, considerando sus elementos constructivos como: ubicación, diseño, paredes y divisiones internas, cielo raso, piso, puertas, ventanas, distribución de espacios, iluminación. Elementos para el control de ambiente, entre los que tenemos la temperatura y humedad, elementos para control de: incendios, inundaciones, terremotos y sabotaje.

El control de acceso es un aspecto muy importante teniendo en cuenta elementos como: identificación de personal, control de acceso y registro de funcionarios del Centro de Informática y otros funcionarios de la Universidad, visitas y vehículos mecanismos de detección de intrusos y vigilancia de las instalaciones.

Otros elementos que se estudiaron y verificaron son: equipos de cómputo, dispositivos de comunicaciones, cableado eléctrico y de datos, conexiones y equipos de respaldo eléctrico; señalando en todos aspectos de identificación, registro, mantenimiento y control.

Aspectos de seguridad en adquisición de software, planeación de proyectos, desarrollo de aplicaciones, Sistemas Operativos, Bases de Datos, Aplicaciones, antivirus, licenciamiento, copias de seguridad, descargas de Internet, correo electrónico, Administración.

Del personal se verificó la capacitación, bienestar laboral y asignación de funciones y responsabilidades.

- *Clasificación de los elementos del Centro de Informática:*

Los elementos anteriormente mencionados se enmarcan dentro de las áreas a auditar: Seguridad de la Red de Datos y de Comunicaciones, Seguridad de la Instalación Eléctrica, Seguridad Física, Seguridad en el Personal y Seguridad Lógica.

- *Entrevistas con el personal:*

Se realizaron entrevistas al Director del Centro de Informática en las que se trataron temas para conocer objetivos a corto y largo plazo, planes de trabajo, actividades, personal, relación con otras dependencias o entidades y necesidades del Centro de Informática, Igualmente, se manejaron temas relacionadas con la seguridad en lo que se refiere al entorno físico, personal, requerimientos de espacios y disposición de equipos.

Se realizaron cuatro entrevistas divididas entre los programadores del Centro de Informática: en la primera se refiere a la asignación de funciones y responsabilidades, actividades realizadas, políticas definidas para el cargo, recursos asignados, áreas de las cuales recibe información y debe reportar, seguridad en la transmisión de información, seguridad en el desarrollo de aplicaciones y capacitación frente a desastres y seguridad informática.

En la segunda entrevista, se tratan temas para la gestión y planeación de proyectos de software, personal participante en el desarrollo de aplicativos, metodologías establecidas para análisis, diseño y programación, control de acceso y privilegios de usuarios para las aplicaciones , tablas de auditoría, procedimientos de prueba y copias de respaldo.

En la tercera entrevista, los aspectos tratados fueron acerca de adquisición de software, legalidad del software, controles antivirus, encriptación de la información, copias de respaldo y restauración del sistema y observaciones al funcionamiento y mantenimiento de la red eléctrica.

En la cuarta entrevista, realizada a los programadores se habló del diseño de la red de datos, mantenimiento a equipos, red de datos y red eléctrica y equipos de respaldo eléctrico, control de acceso de los usuarios a las aplicaciones y administración de cuentas y tablas de auditoría, procedimientos para la creación y almacenamiento de copias de respaldo y aspectos de seguridad del Sistema Operativo.

Se realizó entrevista al Administrador de Internet de la Universidad de Nariño en la que se trataron aspectos de seguridad en los servicios de Internet, desarrollo de aplicaciones, información que se publica, conexiones, tráfico de la red y acceso.

Se realizo entrevistas a los Directores de las de las dependencias de Almacén y Compras, Contabilidad y Presupuesto, Tesorería y Pagaduría y Recursos Humanos, la entrevista manejó temas relacionados con la participación de usuarios en el desarrollo de las aplicaciones de software, disponibilidad del personal del Centro de Informática para atender necesidades, conformidad con las aplicaciones y entrega de reporte, políticas de seguridad internas de cada dependencia en el entorno de trabajo del computador y control de acceso a las instalaciones.

Las entrevistas a las personas auxiliares de las dependencias de OCARA, Almacén y Compras, Contabilidad y Presupuesto, Tesorería y Pagaduría se refirieron a capacitación frente a desastres, acceso a las aplicaciones, capacitación para el manejo del software y controles para el ingreso de datos.

Se entrevistó a la Directora de la Oficina de Control Interno, con el fin de conocer la gestión que se ha realizado frente a una Auditoría de Sistemas en la

Universidad de Nariño, y saber si existe personal especializado en esta área que acompañe los procedimientos de sistematización de la Universidad.

En entrevista realizada a la Jefe de Servicios Generales, se indagó sobre los procedimientos de vigilancia y control sobre ellos, en el Bloque Administrativo y Bloque 1, así como también la capacitación que reciben los vigilantes y los aspectos evaluados de la hoja de vida de cada uno de ellos, para ser contratados.

Se conversó con el Coordinador del Aula de Informática y el Presidente del Comité de Sistemas sobre las licencias de software vigentes en la Universidad y acerca del mantenimiento de equipos y control de software instalado.

Se indagó al funcionario de Servicios Generales encargado del mantenimiento eléctrico de la Universidad, acerca de procedimientos de mantenimientos preventivos y correctivos en la parte eléctrica y atención de solicitudes ante fallos.

- *Observación de operaciones y actuación de los funcionarios:*

Durante las visitas al Centro de Informática y las dependencias observamos cómo interactúan los funcionarios en su entorno informático, verificando la práctica de buenas medidas de seguridad preventivas y de detección.

Se hizo seguimiento a las rondas nocturnas de los vigilantes responsables del Bloque Administrativo y Bloque1, comprobando que su desempeño protejan los activos que se encuentran en las áreas de su responsabilidad.

Las entrevistas se transcriben en el archivo permanente de manera textual, de acuerdo a como se realizaron.

- *Observación de las instalaciones:*

Para una mejor apreciación de las instalaciones y sus elementos se realizó un video en la Oficina del Centro de Informática y las dependencias de OCARA, Almacén y Compras, Contabilidad y Presupuesto, Tesorería y Pagaduría y la Oficina de Recurso Humanos. En este video fueron captadas imágenes de la parte interna y externa de cada una de las oficinas detallando ventanas, puertas paredes, cielo raso, piso, así como su entorno mas inmediato del edificio donde se localizan revisando la existencia de señalización de emergencia y de dispositivos para detección y extinción de fuego, y mecanismos de control de acceso.

Se observa a través del video los puestos de trabajo, ubicación de los equipos y dispositivos de computo, comunicación y eléctricos, distribución de espacios, almacenamiento de papelería, cintas y discos y mobiliario utilizado en las oficinas.

Se observa las conexiones y tendido de cable para la red eléctrica y la red de datos; el estado de los equipos y limpieza al entorno de los equipos y dispositivos de cómputo, comunicaciones, respaldo eléctrico y cableado.

- *Auto documentación:*

Se preparó los cuestionarios de Auditoría como una lista de control (checklist), realizando una lista de los aspectos a evaluar y la verificación de los mismos planteados como: S es si, N no y NA no aplicable, aplicados para las áreas a evaluar Seguridad Física, Seguridad Lógica, Seguridad en redes eléctricas y de datos y Seguridad en Personal.

Se realizaron auto narraciones de las conversaciones con el Coordinador del Aula de Informática y Presidente del Comité de Sistemas, con la Directora de la Oficina de Control Interno, con los vigilantes y con el encargado de mantenimiento eléctrico de la Universidad.

- *Trabajo de campo y ejecución de cuestionarios:*

Se realizaron pruebas de certificación de las conexiones de red con Fibra Óptica y cable UTP del Centro de Informática con las dependencias de OCARA, Contabilidad y Presupuesto, Tesorería y Pagaduría y la oficina de Recursos Humanos.

Se revisaron las conexiones de la red de datos y ponchado de cables, conexiones eléctricas y la codificación de colores de la red eléctrica.

Se revisó el mantenimiento brindado a la red de datos, red eléctrica y equipos de respaldo eléctrico.

Después de revisar todo el entorno de seguridad del Centro de Informática y las dependencias, se registraron los resultados en las listas de control.

- *Recolección de evidencias:*

Se revisó la documentación obtenida entre manuales de funciones, actas, acuerdos, relación de licencias, relación de software, inventario.

Se repasaron las entrevistas a Director y Programadores del Centro de Informática, entrevistas a Jefe y Auxiliares de las dependencias de OCARA, Almacén y Compras, Contabilidad y Presupuesto, Tesorería y Pagaduría y la oficina de Recursos Humanos, entrevista realizada a la Jefe de Servicios Generales de la Universidad de Nariño, de las auto narraciones frente a las conversaciones con el Coordinador del Aula de Informática y Presidente del Comité de Sistemas, con la jefe de la Oficina de Control Interno, con los vigilantes y con el encargado de mantenimiento eléctrico de la Universidad.

Se observo el video del Centro de Informática y de las dependencias de estudio extrayendo las imágenes que señalan vulnerabilidades en puestos de trabajo, ubicación de los equipos y dispositivos de computo, comunicación y eléctricos, distribución de espacios, almacenamiento de papelería, cintas y discos y mobiliario

utilizado en las oficinas, igualmente, conexiones y tendido de cable para la red eléctrica y la red de datos.

Se revisaron los resultados de las pruebas realizadas para la certificación de la red de datos y verificación de las conexiones eléctricas y puntos de red.

Se hizo confrontación de los hallazgos obtenidos durante el desarrollo de los cuestionarios de manera que se respalden con toda la información revisada.

- *Análisis de resultados:*

En base a los resultados obtenidos en la auditoría se detectaron las vulnerabilidades en seguridad y se plantearon recomendaciones para mejorar estos aspectos.

- *Elaboración de archivo corriente:*

El archivo corriente se organizó con los resultados de la investigación registrados en los cuestionarios o listas de control, seguido de los hallazgos, denominación que se dio a las falencias encontradas durante el desarrollo del trabajo de auditoría, cada hallazgo lleva la debida recomendación según el caso y la referenciación de la evidencia.

- *Elaboración de archivo permanente:*

El archivo permanente consta de toda la documentación obtenida, las entrevistas realizadas y auto narraciones.

- *Creación del Informe general y recomendaciones dirigidas al Director del Centro de Informática de la Universidad de Nariño.*

- *Definición de políticas de seguridad:*

Las políticas de seguridad para el Centro de Informática se definieron en base a los resultados obtenidos en la auditoría a través de la cual se identificaron los elementos y vulnerabilidades de los mismos, enmarcados en los mismos aspectos de seguridad física, seguridad lógica, seguridad en red de datos, seguridad en red eléctrica y seguridad de personal.

7. MARCO REFERENCIA

7.1 MARCO LEGAL INSTITUCIONAL

Inicialmente la Universidad tenía contratado los servicios de sistemas con el Centro de Cómputo de Nariño, que era una entidad a la cual estaban asociados Gobernación de Nariño, Alcaldía, Universidad de Nariño y prestaba servicios de sistematización a otras entidades tanto oficiales como privadas y nace la idea de crear el Centro de Informática propio, el Centro de Informática de la Universidad de Nariño se creó por iniciativa de la Facultad de Ingeniería según Acuerdo 010 de 1985, con el fin de promover el mejoramiento y realizar un respaldo a los procesos académicos y administrativos, posteriormente se define esta unidad de sistemas como propia de la Universidad tomando como nombre Centro de Informática de la Universidad de Nariño.

Con un computador Texas Instrument sin disco duro, con dos unidades de disquete de 5 ¼ teniendo como responsable al Ingeniero Delio Gómez, se comenzó a realizar la sistematización dentro de la Universidad comenzando con el proceso de Nómina bajo Dbase2, seis meses después se crea el programa de nómina haciendo pruebas durante tres meses en paralelo con el programa anterior. Mirando la posibilidad de llevar los procesos de sistematización dentro de la Universidad, las directivas hicieron una inversión mayor para dos microcomputadores IBM AT, manejando el Sistema Operativo XENIX y manejador de Bases de Datos Informix. Posteriormente, se trabajó ya con procesos más complejos como matricula financiera, el registro de notas, control de horarios.

Muchos de los fines de la creación de esta dependencia se han transformado de acuerdo con las nuevas necesidades de la Universidad y acompañado de los avances tecnológicos, hoy en día el Centro de Informática trabaja con Unix, esta encargado de apoyar los procesos automatizados de las áreas administrativas y financieras de la Universidad, , compartiendo con la parte académica únicamente lo referente a registro y control académico con el Aula de Informática, siendo el Centro de Informática el puente entre los datos que aparecen en Internet y los datos que se manejan directamente en OCARA. Es así, como el Centro de Informática se responsabiliza de manejar los sistemas correspondientes a Nómina, Tesorería, Cartera, Inventario, Presupuesto, Contabilidad y el Sistema de Control y Registro Académico; información que esta relacionada con estudiantes, docentes, empleados y administrativos.

En la actualidad el Centro de Informática es una dependencia adscrita, según la estructura orgánica de la Universidad, a la Vice-rectoría Administrativa, se encuentra ubicada dentro de las nuevas instalaciones del bloque administrativo, su

estructura interna esta conformada por el Director del Centro de Informática, cuatro programadores y la secretaria.

Dentro de sus funciones se encuentran: desarrollo de programas, mantenimiento a los mismos, mantenimiento de servidores, realizar copias de seguridad, capacitar al personal en las aplicaciones desarrolladas, determinar políticas, planes y programas relacionados con el procesamiento de la información, así como el dirigir, supervisar, promover y participar en los estudios e investigaciones que mejoren la prestación de sus servicios,.

7.2 MARCO TEÓRICO

Seguridad Informática

"Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera infalible. Como esta característica particularizando para el caso de sistemas operativos o redes de computadoras, es muy difícil de conseguir (según la mayoría de expertos, imposible) se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporta tal y como se espera de él) más que de seguridad; por tanto se habla de sistemas fiables en lugar de hacerlo de sistemas seguros".[1]

La seguridad Informática busca mantener la Integridad, Confidencialidad y Disponibilidad de la Información, al igual que también contempla otros aspectos como el control y autenticidad de la información que es manejada por una computadora.

"La integridad de la información es la que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o Auditoría . Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad u Operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede causar severos daños a su dueño (por

[1] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1. p.4.

ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollan producto de características semejantes).

El Control sobre la información permite asegurar que solo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.
La Autenticidad permite definir que la información es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades".[2]

¿Qué se quiere proteger?
Son tres elementos básicos que proteger en un sistema informático hardware, software y los datos. Se define hardware al conjunto de elementos físicos, CPUs, medios de almacenamiento como CDs, disquetes, cintas, cableado, entre otros; Software lo entendemos como el conjunto de programas que hacen funcional al hardware como: Sistemas Operativos y las Aplicaciones, y finalmente como datos se entiende al conjunto de información lógica que maneja el software y hardware.

Ahora, se sabe lo que se debe proteger y sin duda la información es el activo más importante, pero en muchas ocasiones no se estima el valor que realmente merece debido a la intangibilidad de la misma, pero, qué sería de una empresa sin la información?, o qué sucedería si la información no es utilizada adecuadamente? Se plantea estas preguntas en un banco o en una Universidad, entonces, es cuando se comprende la importancia y se da el valor que se merece a la información, por ello se atribuye estas características a la información:

"1. Es crítica: Es indispensable para garantizar la continuidad operativa.
2. Es valiosa: Es un activo con valor en sí misma.
3. Es sensitiva: Debe ser conocida por las personas que la procesan y solo por ellas."[3]

¿De qué se quiere proteger?
Contra el hardware, software y la información pueden haber múltiples ataques, están expuestos a varios elementos que comprometan al sistema lo cual se conoce como amenazas.

Las amenazas pueden ser humanas u ocasionadas por desastres naturales, como también lógicas, si son humanas puede suceder que sean maliciosas manifestadas con ataques externos o internos, o bien pueden ser no maliciosas a

[2] BORGHELLO, Cristian. Tesis "Seguridad Informática: Sus Implicancias e Implementación". Argentina 2001. p. 6.
[3] Ibid. p. 6.

lo que se atribuye errores de los empleados por falta de conocimiento. Entre las amenazas por desastres naturales, incendios, inundaciones y terremotos.

Sin duda el principal el elemento de riesgo para los sistemas son las personas, estas pueden catalogarse como atacantes pasivos cuando se infiltran a un sistema pero no modifican ni destruyen nada y los atacantes activos que son aquellas personas que si causan daño al sistema bien sea a beneficio propio o simplemente por "jugar".

La mayoría de los ataques a una empresa son realizados por el propio personal laborante en ella que aprovechan el entorno de confianza que hay sobre ellas y pueden alterar el sistema, claro esta que muchas veces no se trata de ataque sino de errores accidentales, pero de una u otra manera perjudican al sistema.

En cuanto al personal existe un punto peligroso, y son los empleados que han abandonado su trabajo no a voluntad propia, estas personas pueden valerse del conocimiento que tienen del sistema y de sus vulnerabilidades para alterarlo, con el fin de vengarse.

Al grupo de personas se le añade los curiosos que en muchas ocasiones son estudiantes cuyo deseo es violar la seguridad e ingresar a sistemas no autorizados, por lo general no son destructivos pero igual también pueden causar daño.

Las amenazas lógicas, pueden ser ocasionadas por errores en el código de un programa, por Virus, Gusanos, Caballos de Troya, Bombas Lógicas y muchas técnicas de las cuales uno queda sorprendido.

¿Cómo se debe proteger?

Para proteger un sistema debe realizarse un análisis de las amenazas que pueden afectar el sistema, así como los daños que puede causar y la probabilidad de ocurrencia, una vez determinado esto, se procede a diseñar una política de seguridad que establezca responsabilidades y reglas para minimizar el riesgo de ser perjudicados por alguna amenaza. A los mecanismos utilizados para implementar esta política de seguridad se les denomina mecanismos de seguridad, que se convierten en el elemento que garantizan la seguridad del sistema.

Estos mecanismos son de prevención, detección y recuperación; los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de este, previniendo la ocurrencia de violaciones a la seguridad; los mecanismos de detección son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación y los mecanismos de

recuperación, son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a su funcionamiento correcto.

Seguridad Física

Debido a la importancia que tienen los equipos, programas, instalaciones y la información es necesario que las organizaciones tomen medidas para garantizar la seguridad, para evitar la pérdida o el daño de los mismos.

"Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar en seguridad informática en general; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el software. Hemos de ser conscientes de que la seguridad física es demasiado importante como para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos puede hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada; no importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hallamos definido una política de firewalling muy restrictiva: si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada".[4]

"En cada institución se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado".[5]

Tomando como punto las protecciones físicas, los aspectos que se tienen en cuenta para garantizar la seguridad son:

- Ubicación del centro de cómputo, de manera que su ubicación evite la posibilidad de daños causados por fuego, inundación, explosión, disturbios civiles, amenazas de vecindad, cercanía a instalaciones peligrosas (depósitos de combustible, aeropuertos, minas, etc.)

- Elementos constructivos internos como paredes, puertas, ventanas, suelos, etc., de los cuales el material e instalación, deben garantizar la protección de los recursos informáticos.

---

[4] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1. p.21.
[5] Ibid. p. 21.

- Distribución de áreas o zonas, las cuales deben hacerse según la utilización y el valor de los activos que resguardan, pueden distribuirse de acuerdo con estos criterios:

  - Áreas Públicas, espacios en los que no hay ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.

  - Áreas Internas, espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización con motivos relacionados con la institución. Pueden haber en ellos recursos informáticos con un valor bajo.

  - Áreas de Acceso Limitado, espacios cuyo acceso esta reservado a un grupo reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito. Pueden concentrarse en ellos recursos informáticos, que en conjunto tienen un valor medio.

  - Áreas de Acceso Restringido, espacios cuyo acceso esta reservado a un grupo muy reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por actividades propias de la organización. En ellos se concentran recursos informáticos que en conjunto tienen un alto valor o contienen información crítica o confidencial de la empresa.

- Control ambiental, un centro de cómputo debe estar provisto de mecanismos de ventilación, aire acondicionado y calefacción, que regulen las medidas de temperatura y humedad adecuada para evitar el deterioro de los equipos y preservar la salud de los operarios.

- Seguridad frente a desastres, este tipo de seguridad cubre amenazas como incendios, inundaciones u otro tipo que sean ocasionadas por la naturaleza o por el hombre.

Los incendios se ocasionan principalmente por fallas en la instalación eléctrica, por el uso inadecuado de combustibles o la inadecuada manipulación y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad, es considerado el enemigo número uno de los sistemas de información ya que destruye fácilmente computadores, archivos y programas.

Es importante dotar al centro de cómputo, con sistemas de detección y extinción de incendios adecuados según el tipo de fuego que se puede presentar en el área.

- Control de Acceso, deben mantenerse controles de acceso efectivos en proporción de los recursos humanos y del valor de los equipos y de la información que se resguarda, los pueden haber de muchas formas: llaves, sistemas

electrónicos, guardas de seguridad, etc., lo importante es que cualquiera que sea, permita controlar el acceso únicamente a personal autorizado y que se registre la entrada y salida del personal, de manera que estos registros hagan auditable la operación de acceso a las instalaciones.

- Copias de respaldo, lo primero que se debe tener en cuenta en una empresa cuando se habla de seguridad, es tener respaldo de la información, de manera que permita seguir operando, es por ello que se deben establecer políticas de Backup de los datos y de los programas de la empresa y guardarlas en lugares seguros dentro y fuera del sitio.

- Seguridad en equipos, los computadores y equipos de comunicaciones como cualquier máquina pueden sufrir daños que pueden dejar a la empresa sin servicio, es por esta razón que deben existir planes de mantenimiento preventivo adecuados, y que se efectúen por personal especializado.

Seguridad Lógica

La seguridad lógica para garantizar la integridad, confidencialidad y disponibilidad de la información, abarca las siguientes áreas:

- Controles de acceso, la seguridad lógica, esta orientada a establecer los controles de acceso que se deben tener para proteger la información almacenada al igual que controlar el mal uso de la información, un inadecuado control de acceso lógico es una amenaza potencial para la pérdida o divulgación de la información.

"La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos , a los programas de uso generadle uso específico, de las redes y terminales.
La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocerle momento en que se produce un cambio o fraude en los sistemas".[6]

- Desarrollo de Software, el desarrollo de software debe partir con una adecuada planeación y esta debe ser revisada y autorizada al nivel que su importancia lo requiera. Se debe considerar otro aspecto como es la integridad en las líneas de código de un programa, ya que puede tener alguna rutina que elimine o modifique algún tipo de archivo, es por eso que debe participar personal de Auditoría que verifique la ausencia de "Caballos de Troya, bombas lógicas o algún otro tipo de líneas maliciosas, igualmente que verifiquen la calidad del programa.

- Todos los programas deben contemplar logs, pistas o controles de auditoría.

[6] ECHENIQUE, José Antonio. Auditoría en Informática. McGrawHill. Segunda Edición. México.p.195

▪ Sistemas Operativos, estos programas configurados correctamente generan seguridad, puesto que manejan y controlan la ejecución de programas de aplicación y proveen los servicios que estos programas requieren, dependiendo del usuario y del sistema que este trabajando.

▪ La seguridad del software manejador de bases de datos, se usa para restringir el acceso a un usuario específico, a determinados archivos, registros, procedimientos y funciones.

▪ Encriptamiento, encriptar es proteger la información por medio de un algoritmo de manera que esta no pueda ser leída normalmente. El objetivo es asegurar la privacidad y mantener la información alejada de personal no autorizado.

▪ Seguridad en contra de Virus, para evitar pérdida o variaciones en la información causado por software antivirus, se deben utilizar únicamente paquetes originales y prohibir la lectura de medios externos sin ser revisados previamente.
Todos lo computadores deben tener analizadores y desinfectadores de virus instalados y actualizados.

▪ Legalidad del Software, el software que se utilice debe ser únicamente el autorizado por la empresa, para evitar sanciones legales.

Seguridad en Comunicaciones y Redes
La protección de los equipos conectados en red y de los datos que almacenan y comparten, es uno de los aspectos más importantes en la interconexión de equipos, pero la seguridad en una red es mucho más que evitar accesos no autorizados a los equipos y a sus datos.

La seguridad en una red incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red, por lo cual es vital establecer mantenimiento preventivo para evitar la pérdida de datos y minimizar los fallos en la red.

En un entorno de red debe asegurarse la privacidad de los datos sensibles y también las operaciones de la red de daños no intencionados o deliberados.

El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio.

Las principales amenazas que afectan la seguridad de los datos en una red son.
- Acceso no Autorizado.
- Soborno electrónico.

- Robo.
- Daño intencionado o no intencionado.

La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red.

Cortafuegos (Firewall)
Un cortafuego es un sistema de seguridad en una red, por lo general es una combinación de hardware y software, que esta destinado a proteger la red frente a amenazas externas que proceden de otra red, incluyendo Internet.

Los cortafuegos evitan que los equipos de red de una organización se comuniquen directamente con equipos externos a la red, y viceversa.
Los cortafuegos auditan la actividad de la red, registrando el volumen de tráfico y proporcionando información sobre los intentos no autorizados de acceder al sistema.

Estándares
Siendo las redes un medio de comunicación, los fabricantes establecen unos parámetros para que los productos puedan interactuar, es así como la necesidad de una estandarización se ha incrementado, cuando se mantienen estos estándares, es posible la comunicación entre productos hardware y software de diversos fabricantes.

A través de la familia del estándar *IEEE 802,* se fundamenta, controla y verifica las normas básicas para el correcto y eficiente funcionamiento de las redes de datos.

Seguridad en el Personal
Para conseguir una seguridad efectiva y completa de los recursos informáticos incluyendo la información, es preciso delimitar las funciones y definir responsabilidades de quienes lo utilizan, es claro que los recursos informáticos y la información son propiedad de la empresa, pero se hace necesario delegar entre los trabajadores que desempeñan diferentes funciones la protección de los recursos, asignando a cada uno de ellos sus responsabilidades.

Todos y cada uno de los recursos informáticos y la información, deben tener una persona responsable, asignada por la dirección, estableciendo segregación de responsabilidades a las personas adecuadas con el fin de disminuir el riesgo de mal uso accidental o deliberado del sistema.

“En muchas ocasiones el mayor riesgo de fraude o mal uso de la información está dentro del mismo personal, y la mayor seguridad esta en contar con personal leal,

honesto y con ética. Para lograr esto se debe contar con personal capacitado, motivado y con remuneraciones adecuadas".[7]

Ahora, así como se asegura la protección de los recursos informáticos y de la información, es muy importante proteger al personal que se encuentra responsable de los mencionados elementos, entonces, se debe tener en cuenta la ergonomía.

"La Ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible"[8]

La Ergonomía establece la manera como los métodos, los objetos, las maquinarias herramientas e instrumentos o medios y las condiciones de trabajo, de tal manera que no afecten a la anatomía, la fisiología y la psicología de los trabajadores; su aplicación se encuentra orientada, a la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas trastornos óseos o musculares, trastornos visuales y el envejecimiento prematuro.

Políticas de Seguridad

Políticas de seguridad es un conjunto de reglas que adopta una organización para aumentar el nivel de seguridad del sistema informático y así garantizar la protección de la información.

Las políticas de seguridad tienen dos propósitos fundamentales, una es informar a los usuarios de las obligaciones que tienen respecto a la seguridad y otra es dar guías para actuar ante posibles amenazas o problemas presentados.

Cualquier política de seguridad debe contemplar los tres elementos claves de seguridad: Integridad, Disponibilidad y Confidencialidad.

Un esquema de políticas de seguridad requiere alto compromiso de la organización tanto de directivas como otros funcionarios, para establecer las fallas y debilidades y actualizar las políticas de acuerdo al nuevo ambiente tecnológico en que se vea rodeada la organización.

Estándares de Auditoría.

A través de estos documentos se logra valorizar, optimizar y reforzar los trabajos de Auditoría y control interno de la instituciones, los siguientes estándares han servido como base para la definición de políticas:

---

[7] ECHENIQUE, José Antonio. Auditoría en Informática. McGrawHill. Segunda Edición. México.p.219
[8] ALDEGANI, Gustavo Miguel. Seguridad Informática. MP Ediciones. Argentina 1997. p.30

COBIT (Control Objectives for Information and related Technology)
Se encuentra enfocado a los auditores de sistemas. Este documento se presenta como uno de los estándares para el control de Tecnología Informática.

INFORMATION SECURITY POLICIES (Políticas de seguridad de la información)
A través de este documento se logra una visión y orientación clara sobre los procedimientos a seguir en la creación de políticas de seguridad.

NORMA TECNICA COLOMBIANA NTC-ISO 9000-3
Documento que establece las normas de administración y aseguramiento de la calidad aplicada al desarrollo, suministro, instalación y mantenimiento de software de computadores.

NORMA ISO/IEC1779
Instrumento para la Gestión de la seguridad de la Información de una forma completa, efectiva y ordenada y aporta una visión global del problema de la seguridad, asegura la disponibilidad de información, confidencialidad, buen uso e integridad, implica a todo el ente a auditar.
Los objetivos de esta norma son cuatro:

1. "Atender la demanda de las empresas relativa al desarrollo, implantación y medida de prácticas de seguridad efectivas. Seguridad propia y en relación con otras organizaciones, estableciendo un marco referencial común que establezca las bases para la confianza mutua en seguridad de la información.
2. Proporcionar principios y recomendaciones de gestión en los que basa la política de seguridad.
3. Conseguir la seguridad definiendo controles proporcionales al riesgo.
4. Identificar controles de aplicación general independientes del tamaño y la tecnología de la empresa".

ORANGE BOOK
Este documento define mecanismos para la protección de la información, y medir la confiabilidad de los sistemas, en base a normas establecidas por el Gobierno de los E.E.U.U.

CRAMM
Herramienta para la evaluación de riesgos, niveles de ocurrencia de amenazas y vulnerabilidades, impacto en activos. Utilizando cuestionarios, matriz de riesgos. Contramedidas, priorización, base de datos de controles de seguridad, ayudas y reportes.

COBRA
Herramienta para identificación, evaluación de amenazas y vulnerabilidades. Empleando cuestionarios, encuestas de riesgos y reportes. Bases de conocimiento, personalización y administrador de módulos.

NORMA TÉCNICA NTC 3560
Guía para la adquisición de sistemas de computación, sistemas de procesamiento de la información, procedimientos y desarrollo.

NORMAS ISO SOBRE SEGURIDAD: ISO 13335,
Directrices para la Gestión de la Seguridad, criterios para la Evaluación de la Seguridad de las tecnologías de la información.

EIA/TIA 568
Recomendaciones para sistemas de Cableado Estructurado

NBE/CPI-96
Norma Básica de Edificación

8. PLAN GENERAL

SEGURIDAD LÓGICA

- Verificar la seguridad en el manejo de software.
- Determinar la seguridad en el control de acceso lógico.
- Verificar la administración de las copias de seguridad.
- Determinar la seguridad implementada en los procesos de desarrollo se software.

SEGURIDAD EN EL PERSONAL

- Verificar que las funciones establecidas en el manual de funciones, se encuentran acorde con las actividades realizadas por los funcionarios.
- Determinar la capacitación de los funcionarios en procesos de seguridad física y lógica.
- Verificación de controles de acceso a personal.

SEGURIDAD FÍSICA

- Determinar los lineamientos de seguridad física con los cuales esta dotado el Centro de Informática.
- Verificar el estado de la seguridad en instalaciones del Centro de Informática.
- Identificar vulnerabilidades frente a posibles ataques o desastres.
- Determinar las medidas de seguridad establecidas para los equipos.

SEGURIDAD DE LA INSTALACIÓN ELÉCTRICA

- Determinar el estado de las instalaciones eléctricas del Centro de Informática y las dependencias a las que presta sus servicios.

- Verificación de sistemas de respaldo.

SEGURIDAD DE LA RED DE DATOS Y LAS COMUNICACIONES

- Determinar el estado de las redes de datos del Centro de Informática y las dependencias a las que presta sus servicios.

- Identificar los servicios de comunicaciones que presta el Centro de Informática.

- Verificar los controles de acceso a través de las redes de datos.

9. INFORME GENERAL

Fecha: San Juan de Pasto, Mayo 23 de 2005-05-23

Para: Director Centro de Informática

Asunto: Auditoría a la Seguridad Física, Lógica y de Personal del Centro de Informática.

El propósito general de la Auditoría , es diagnosticar el manejo de la seguridad que se tiene en el Centro de Informática, con el fin de determinar el estado actual de la misma y en base al análisis de seguridad, generar un documento de Políticas de Seguridad Informática para esta dependencia.

La Auditoría se desarrolló en base a los aspectos determinantes en la seguridad, como los son el **Aspecto Físico** vinculando dentro de este, la construcción, control de ambiente, control de acceso, desastres, equipos; **Aspecto Eléctrico** en el que se contempló, los circuitos eléctricos, puesta a tierra, mecanismos de respaldo, otro de los aspectos que se examinó es las **Redes de Datos**, en el cual se trabajo sobre cableado y dispositivos, mantenimiento y servicios de las redes de datos, el siguiente aspecto cubierto fue la **Seguridad de Personal**, en el que se tubo en cuenta capacitación de los usuarios, responsabilidades de los mismos, controles de acceso y por último se contemplo la **Seguridad Lógica**, tema que comprende desarrollo de aplicaciones, antivirus, copias de seguridad, Sistema Operativo y herramientas de software.

Para el desarrollo de la auditoría, se utilizaron principios de Auditoría de aceptación general, normas de Auditoría , colaboración de personal experto, procedimientos y técnicas, con el fin de recolectar evidencia razonable y suficiente sobre los hechos, evidencias de la evaluación, aplicados en el Centro de Informática y las dependencias a las cuales presta servicio (OCARA, Tesorería, Recursos Humanos, Almacén, Internet).

La Universidad de Nariño cuenta con funcionarios con gran experiencia en las actividades que realizan y en los cargos que desempeñan, quienes además cuentan con las herramientas suficientes para cumplir sus tareas, de manera especial el Centro de Informática esta equipado con un grupo de trabajo idóneo para el cumplimiento de los objetivos de esta dependencia.

En la evaluación de la seguridad al Centro de Informática se encontraron deficiencias en:

Aspecto Físico

- Frente a la ubicación y construcción, el Centro de Informática presenta problemas al encontrarse en un primer piso, se hace mas vulnerable a posibles accesos no autorizados que se pueda realizar a través de las ventanas que no son las adecuadas para proteger, contra accesos forzosos ya que los antepechos se sujetan de manera sencilla a las paredes del edificio y son fácilmente extraíbles con una palanca y ni las ventanas, ni las puertas cuentan con mecanismos de detección de intrusos, además la puerta principal de acceso al Bloque Administrativo donde se encuentra el Centro de Informática, no esta protegida por antepecho metálico lo que permite un posible acceso no autorizado, a esto se une que el Bloque Administrativo no cuenta con un vigilante dedicado de tiempo completo a la protección de este Bloque, y que su turno de vigilancia comprende además del Bloque Administrativo la Biblioteca y la Zona del Auditorio, situación que compromete a la seguridad física del Centro de Informática.

  En lo referente a su distribución se encontro que no adecuado para el cumplimiento de sus actividades y protección de las áreas. La distribución actual no permite realizar una adecuada atención al público y mantener un control de acceso a las áreas que se consideran restringidas, igualmente no dispone de espacio suficiente, para asignar un sitio adecuado para el almacenamiento de papelería, discos y cintas y para realizar procesos de mantenimiento.

- Frente al control ambiental el Centro de Informática no cuenta con mecanismos de monitoreo de temperatura y humedad que le permitan realizar un seguimiento y prevenir posibles problemas que afecten el funcionamiento de los equipos y el bienestar del personal. El cuarto de máquinas no cuenta con un sistema de aire acondicionado que mantenga una temperatura ambiente constante.

- En lo que se refiere a desastres, el Centro de Informática presenta problemas en los temas relacionados con incendios, ya que no cuenta con mecanismos detectores que permitan advertir de estos incidentes, además cuenta con inmobiliario, cortinas, módulos de trabajo y papeleras de materiales combustibles que facilitan la propagación del fuego; igualmente el Centro de Informática no cuenta con elementos como extintores de tipo y capacidad adecuada para controlar y apagar incendios; el gabinete de incendios que se encuentra en el primer piso del edificio, no sería suficiente para controlar un incendio.

En lo relacionado con inundaciones no se cuenta con equipos como moto bombas para la evacuación de agua, y el Centro de Informática se encuentra cercano a un hidrante que en caso de presentarse un daño en este elemento podría ser perjudicial para los equipos y papelería del Centro de Informática, contando con que muchos de estos elementos se encuentran a nivel del suelo.

Ni la Oficina del Centro de Informática, ni el Bloque Administrativo cuentan con señalización que indiquen salidas de emergencia y no se encuentran a disposición teléfonos de emergencia.

- En relación con la dotación de equipos, no se cuenta con una cantidad adecuada de equipos para el procesamiento de la información, ni con un equipo de respaldo en caso de que el servidor presentara algún tipo de inconveniente, los equipos no cuentan con un mantenimiento preventivo periódico.

  En el Centro de Informática y el Bloque Administrativo no existe un control de ingreso y salida de equipos que evite la circulación no autorizada de los mismos. Por otra parte, dentro de los aspectos que perjudican a los equipos, se tiene que el Centro de Informática no recibe una limpieza adecuada dada la disposición de los equipos y elementos de red que no lo permiten.

Aspecto Eléctrico

- Frente a la red eléctrica, el Centro de Informática no cuenta con pararrayo, los circuitos eléctricos no se encuentran etiquetados especificando si son regulados o no regulados y pertenecen a UPS o si están aterrizados, además se presentan estabilizadores y multitomas con sobre carga de equipos descompensando así los circuitos eléctricos, algunos equipos no se encuentran conectados a circuitos regulados ni aterrizados, se presentan conexiones de cables y tomas que no están adecuadamente conectadas colocando en riegos los equipos frente a posibles corto circuitos.

- Frente al mantenimiento eléctrico, no se realiza un mantenimiento preventivo periódico a los circuitos eléctricos y a la puesta a tierra, no se lleva registro de los mantenimientos correctivos ni los daños que ocurren en los circuitos.

- Frente a los sistemas de respaldo de energía, el Centro de Informática no cuenta con un sistema ininterrumpido de energía como planta eléctrica de combustible que permita continuar las labores normales cuando se trate de una suspensión prolongada del fluido eléctrico.

Aspecto en Redes de Datos

- Frente a la administración, no se encuentra un diseño de la red de datos actual del Centro de Informática y de las dependencias a las cuales presta su servicio, así como no existe un documento que relacione la ubicación de equipos y dispositivos.

  Los dispositivos y equipos no se encuentran en lugares en donde sea restringido el acceso a personal no autorizado.

  Se presenta problemas en la disposición del cableado, ya que están en varios tramos que no se encuentran protegidos por canaleta, existen algunos puntos de red sus terminales no están correctamente instalados. Los equipos no cuentan con Patch Cords y los terminales de los cables no se encuentran correctamente instalados presentando así cables sueltos.

- Frente al mantenimiento, los dispositivos y cableado no recibe mantenimiento preventivo periódico y los resultados del mantenimiento correctivos y fallos ocurridos no se registran y los equipos que presentan fallas no se remplazan.

Aspecto de Personal

- En lo que se refiere a la capacitación de personal, se encontró que los usuarios finales no cuentan con un manual de usuario que les permita resolver problemas de manejo que se puedan presentar. Además, los funcionarios no conocen claramente el manual de funciones, los cuales se encuentran desactualizados, a razón de esto los funcionarios realizan tareas que no son propias de su cargo.

- Frente al ingreso de personas, no existe un control electrónico para el control de acceso a las oficinas o lugares restringidos, los funcionarios no portan un carné que establezca su identidad, cargo y dependencia, no se realiza un control de entrada de visitantes que registre nombre, motivo, fecha y hora, ni se le asigna un carné que los identifique como visitantes.

  Al finalizar los contratos laborales de los trabajadores no se toman medidas de seguridad para prevenir posibles accesos posteriores mal intencionados al sistema.

El Centro de Informática no esta dotado con mecanismos de seguridad para detección de intrusos, considerando que tiene vulnerabilidades en elementos de acceso como puerta y ventanas.

- La vigilancia que se presta al Centro de Informática, no es adecuada ya que no se tiene un vigilante exclusivo para esta dependencia o bloque, y el personal que existe no cuenta con la suficiente capacitación para el manejo de acceso no autorizado.

Frente a la Seguridad Lógica

- Frente al desarrollo se plantean algunos inconvenientes en las diferentes fases, como no realizar una delimitación y restricción de los sistemas a desarrollar en tiempo y recursos, la falta de tiempo y personal hace que no se contemple documentación completa en las fases de desarrollo, generando ausencia de Manuales Usuario, Análisis, Diseño, con lo cual siempre se va a depender de un persona para administrar, adecuar o modificar un desarrollo. También se encontró que en ninguna de las etapas participa personal especializado en seguridad, ni personal de Control Interno que realice seguimiento a la aplicación, realice las pruebas de seguridad o examine la codificación.

  En la programación se presentan problemas con el manejo de contraseñas ya que las aplicaciones no cuentan con opciones para la realización de cambios de contraseñas desde el menú de los usuarios, ni mensajes que adviertan de la necesidad de hacerlo.

  La seguridad de las contraseñas, esta expuesta ya que no se guardan encriptadas.

  No existen estándares para la programación con lo cual cada programador establece sus propios lineamientos y es él la única persona que puede realizar modificaciones a los programas, además, se dificultan los mecanismos para realizar seguimiento a las aplicaciones.

- En lo que se refiere a copias de seguridad, los inconvenientes se presentan a que no existen lugares apropiados para el almacenamiento de los medios que contienen las copias, con lo cual se facilita su acceso y se complica el control de las mismas, además, no existen procedimientos por escrito que establezcan los pasos o tareas a realizar en caso de hacerse necesaria la restauración de alguna de ellas.

- Frente a los requerimientos legales: se presentan problemas en el control de software instalado en los computadores, el Sistema Operativo que maneja el Centro de Informática no cuenta con licencia de uso.

- En el manejo de antivirus: los tiempos de actualización de los antivirus son demasiado largos para evitar posibles contagios, además, no se están actualizando el software con los parches y actualizaciones que generan los proveedores o desarrolladores de manera constante. No existe una restricción para la descarga de archivos de Internet.

- En cuanto a inconvenientes con las bases de datos, se encuentra que la información que se almacena no esta encriptada por ningún mecanismo de encriptación. A pesar que se realizan copias de seguridad de la información que se aloja en las bases de datos, no se encuentran procedimientos por escrito que establezcan los pasos a seguir en el caso de una restauración.

- Frente a los Servicios de Internet, el proveedor de Internet no ofrece mecanismos de seguridad que minimicen los posibles ataques que se puedan presentar por este medio, la oficina de servicios de Internet no cuenta con unos lineamientos por escrito que establezcan los parámetros que se deben tener en cuenta por las personas que realizan el desarrollo de aplicaciones orientadas a la Web para garantizar la seguridad en los servidores y servicios de Internet, dado que esta oficina no cuenta con personal suficiente para todas sus actividades no se realiza un seguimiento a las aplicaciones que se desarrollan por personas ajenas a la oficina como estudiantes.

Los hechos anteriormente planteados son el resultado del trabajo aplicado en el Centro de Informática como eje central de los procesos tecnológicos, y en las dependencias con las cuales tiene relación, encontrado en líneas generales inconvenientes en la capacitación de los usuarios, problemas de tipo eléctrico y en redes de datos, que de alguna u otra manera incrementan los riesgos asociados con la seguridad informática dentro de la Universidad, pero lo mas importante de resaltar, es la falta de concientización general de los funcionarios en la importancia de la seguridad informática y en el cuidado que se debe tener en el manejo de los recursos de la información, principalmente la información que es la base fundamental del funcionamiento de la Academia .

Es por esta razón, que es de suma importancia la conformación de un equipo especializado para el apoyo administrativo y tecnológico, que tenga suficiente capacitación, criterio y autonomía en lo relacionado con la seguridad, el cual debe realizar seguimientos exhaustivos, desde el mismo proceso de planeación de los aplicativos, pasando por su codificación y la llegada del programa al usuario final, así como en la implementación y crecimiento de la infraestructura tecnológica de la Universidad de Nariño.

10. CONCLUSIONES AUDITORÍA

- El Centro de Informática cuenta con personal calificado para el desarrollo de las actividades que desempeñan y que han demostrado responsabilidad, alto grado de compromiso y ética, lo cual brinda cierta seguridad de que los procesos de desarrollo y administración de los sistemas de información, bases de datos programación y demás se desarrollan a conciencia y con ciertas normas de seguridad.

- De igual manera, se puede expresar de los funcionarios que operan los sistemas desarrollados, quienes a pesar de mantener bajos niveles de seguridad, respaldan con su compromiso y ética la información y programas que manejan.

- Los grados de confianza y compromiso de los trabajadores son puntos a favor del sistema actual, sin embargo, no son suficientes para afrontar los peligros tecnológicos con los que cuentan los sistemas de hoy en día, ni con las generaciones de estudiantes modernos, que son cada vez más inquietos y curiosos de la los procesos sistematizados y se debe pecar por exceso de confianza pensando que como las situaciones no se han presentado hasta ahora o que si lo han hecho no han afectado de manera significativa, nunca lo van a hacer, es por eso que se deben adoptar las medidas correctivas y preventivas necesarias, seguir las recomendaciones y profundizar los estudios para cada vez mejorar los niveles de seguridad.

- De la misma manera que se deben establecer controles lógicos a los sistemas, también se debe implementar medidas de control y aseguramiento físico, por que es muy fácil hoy en día transitar con computadoras, discos duros, u otros dispositivos por cualquier rincón de la Universidad, sin tener ningún tipo de restricción y sin saber cual es el origen o el destino que tendrán esos dispositivos. De ahí la importancia de reforzar con personal capacitado la vigilancia y control dentro de las áreas más delicadas como el Centro de Informática.

- La capacitación es uno de los pilares del mundo moderno y es la mejor manera de llegar a los trabajadores para crear en ellos una conciencia de seguridad y control, reduciendo así las vulnerabilidades con las que se cuenta es estos momentos. Además establecer que la capacitación en seguridad informática es un tema de actualización constante, debido a que la tecnología esta avanzando día a día y que los procesos de seguridad deben ir a la par de esos avances.

Es por esto que el personal que desarrolla aplicaciones, presta servicios en redes, eléctricos, acceso, y hasta las mismas estructuras físicas deben estar preparadas,

en constante retroalimentación y actualización para afrontar las nuevas modalidades de ataques y los nuevos riesgos tecnológicos.

- Si bien es cierto, los procesos de mejoramiento son necesarios y cuando hablamos de seguridad se hacen obligatorios, estos debe hacer parte de un procesos de reestructuración no solo mental sino también de tipo administrativo, quienes deben ser los primeros en tomar conciencia de la necesidad de mejorar la seguridad, y quienes deben crear los espacios y brindar los recursos económicos y de personal para lograr el objetivo que será que la seguridad llegue de manera segura a la Universidad.

11. POLÍTICAS DE SEGURIDAD PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

11.1 INTRODUCCIÓN

Las políticas de seguridad son mecanismos por los cuales las instituciones, establecen lineamientos claros que llevan a un mejor funcionamiento; la seguridad informática hace referencia a procedimientos de seguridad preventivos y correctivos que las entidades deben mantener frente a posibles problemas que comprometan el funcionamiento de la institución, la unión de estos dos temas ha sido muy poco tratada dentro de las entidades, y cuando se lo ha tomado en cuenta no se ha enfatizado de manera óptima para resolver problemas y estar preparados para afrontarlos.

Es así como el siguiente documento se convierte en la base de un modelo de seguridad, que lógicamente no garantiza cien por ciento que no se presente ataques, ni problemas de seguridad, pero si minimizan, regulan y orientan las acciones, compromisos y lineamientos que la Universidad debe tomar para reducir los riesgos relacionados con la seguridad informática, permitiéndole aumentar la confianza frente a la integridad, confidencialidad y disponibilidad de la información. Este es el resultado de un estudio de la identificación de los elementos que intervienen en los procesos que realiza el Centro de Informática, y de las vulnerabilidades que presentan estos elementos que pueden afectar el cumplimiento de las funciones de la Universidad, es así como teniendo conocimiento de la importancia de los procesos que realiza la Universidad, se definió políticas de Seguridad Informática enmarcadas en aspectos de Seguridad Física, Seguridad Lógica, Seguridad de la Red de Datos, Seguridad de la Red Eléctrica y Seguridad de Personal, que minimicen el riesgo ante posibles amenazas y garanticen la integridad, disponibilidad y confidencialidad de la información.

11.2 CONTENIDO POLÍTICAS DE SEGURIDAD PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO.

1. SEGURIDAD FÍSICA

1.1. Construcción de Instalaciones físicas

1.1.1 Ubicación
1.1.2 Distribución de Áreas
1.1.3 Diseño
1.1.4 Paredes y Divisiones
1.1.5 Piso y Cielo Raso
1.1.6 Puertas
1.1.7 Ventanas
1.1.8 Iluminación

1.2 Control de Ambiente.

1.2.1 Temperatura
1.2.2 Humedad

1.3 Seguridad Frente a Desastres

1.3.1 Incendios
1.3.2 Inundaciones
1.3.3 Terremotos
1.3.4 Sabotaje
1.3.5 Emergencias

1.4 Control de Acceso a las instalaciones.

1.4.1 Control de Acceso a Funcionarios del Centro de Informática
1.4.2 Control de Ingreso y Salida de Visitas
1.4.3 Control de Ingreso y Salida de Vehículos
1.4.4 Vigilancia

1.5 Seguridad Equipos de Cómputo

1.5.1 Registro
1.5.2 Mantenimiento

1.6 Copias de seguridad

SEGURIDAD REDES ELÉCTRICAS

2.1 *Redes Eléctricas*

2.1.1 Puesta a Tierra
2.1.3 Mantenimiento

2.2 *Respaldo Eléctrico*

2.2.1 UPS y Planta Eléctrica

SEGURIDAD REDES DE DATOS

3.1 *Red Física*

3.1.1 Dispositivos y Conexión
3.1.2 Diseño

3.1.3 Mantenimiento
3.2 *Servicios*
3.2.1 Recursos De Red
3.2.2 Internet
3.3 *Lógica*
3.3.1 Servidores
3.3.2 Muros de fuego (Firewall)
3.3.3 Monitoreo

SEGURIDAD LÓGICA
4.1 Proyectos de Software
4.1.1 Planeación del Proyecto
4.1.2 Definición de Seguridad
4.1.3 Desarrollo de Software
4.2 *Adquisición de Software*
4.2.1 Compra de Software
4.2.2 Outsourcing
4.3 *Control de Acceso*
4.3.1 Utilización de los Sistemas
4.3.2 Identificación y Autenticación de Usuarios
4.3.3 Control de Usuarios
4.3.4 Especificaciones de Contraseña
4.3.5 Vigencia de Contraseña
4.3.6 Entrada y Transmisión de la Contraseña
4.3.7 Periodo de Autenticación
4.4 *Protección Antivirus*
4.4.1 Antivirus
4.5 *Requerimientos Legales*
4.5.1 Licencias

5. SEGURIDAD EN EL PERSONAL
5.1 *Funciones y Responsabilidades*
5.2 *Capacitación del Personal*
5.3 *Ergonomía*

1. SEGURIDAD FÍSICA	
Aspecto:	1.1. Construcción de Instalaciones físicas
Elemento:	1.1.1 Ubicación
El Centro de Informática de la Universidad de Nariño debe ubicarse en una área interna de la Universidad, distante de la calle y libre de alto tráfico de personas.	
El Centro de Informática debe ubicarse en un lugar que no tenga acceso desde la parte externa del edificio.	
La ubicación del Centro de Informática debe ser lo mas cerca posible a las áreas a las cuales presta el servicio.	
La localización del Centro de Informática debe ser en un sitio exento de la influencia de señales de radar, para evitar la interferencia en el procesamiento electrónico de la información.	
El Centro de Informática de la Universidad, no debe situarse cerca de áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.	
La edificación donde se sitúa el Centro de Informática, debe ser un sitio retirado de grandes corrientes de agua.	
El Centro de Informática debe ubicarse en un área distante de tuberías de agua, desagües, hidrantes, grifos o aspersores contra incendio.	
Las instalaciones del Centro de Informática deben ubicarse en un sitio donde el suelo no se encuentre sometido a vibraciones como las producidas por maquinaria pesada o tráfico de transporte de carga.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1. Construcción de Instalaciones físicas
Elemento:	1.1.1 Ubicación
El parqueadero debe ubicarse fuera del área perimetral del edificio del Centro de Informática.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.2 Distribución de Áreas
La dependencia del Centro de Informática se distribuirá internamente en áreas públicas, áreas de acceso limitado y áreas de acceso restringido, de acuerdo con su utilización y el valor de los activos que resguarden.	
El Centro de Informática se distribuirá en dos pisos, el primero dispuesto para el área pública y el segundo para las áreas limitada y restringida.	
El área pública será establecida especialmente para atención al público y recibo de visitas de carácter laboral o afines, para funcionarios del Centro de Informática.	
En el área pública se localiza la oficina del Director, la oficina de la secretaria y sala de recibo.	
El área de acceso limitado comprende el área operativa, se establece para los sitios de trabajo de los funcionarios del Centro de Informática, sección de mantenimiento y bodega.	
El ingreso al área de acceso limitado debe realizarse a partir del área pública del Centro de Informática, no se debe acceder de una parte externa a las instalaciones.	
En el área de acceso restringido se concentrarán los servidores, dispositivos de comunicaciones y dispositivos o equipos que contengan información confidencial y de carácter crítico para el desarrollo de las actividades del Centro de Informática.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.2 Distribución de Áreas
En el área de acceso restringido se ubicara el cuarto de máquinas, la discoteca y cintoteca.	
El ingreso de funcionarios del Centro de Informática a las áreas de acceso limitado y áreas de acceso restringido, se debe realizar a través de dispositivos electrónicos que faciliten el control de acceso y su registro.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.3 Diseño
Para la construcción del edificio donde se ubique el Centro de Informática, debe realizarse un completo estudio de suelos, que determinen la capacidad portante de resistencia, para evitar posibles hundimientos de la estructura por razones de sobrepeso.	
Para el edifico donde se ubica el Centro de Informática, debe realizarse el diseño estructural el cual debe cumplir con la Norma de Sismo Resistencia NSR-98.	
Será el Director del Centro de Informática en conjunto con el consultor para el diseño arquitectónico, quienes establezcan el mapa de espacios, y disposición de la red de datos y red eléctrica para el Centro de Informática.	
El diseño del Centro de Informática debe considerar también la incorporación de sistemas de seguridad como alarmas, circuito cerrado de televisión o cualquier otro tipo de dispositivos electrónicos, según el grado de seguridad del sitio.	
El Director del Centro de Informática deberá revisar los planos que contemplen la distribución de áreas, planos de la red de datos y red eléctrica, de manera que cumplan con los requerimientos establecidos por el Centro de Informática.	
El diseño arquitectónico debe cumplir con el Plan de Ordenamiento Territorial, POT.	
El profesional encargado del diseño del Centro de Informática, debe presentar estudio de suelos, planos estructurales, planos arquitectónicos, planos de la red de datos y red eléctrica, debidamente aprobados.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.3 Diseño
El Centro de Informática debe mantener una copia de los planos de la red de datos y red eléctrica de ésta dependencia y de las demás dependencias a las cuales presta el servicio, con el ánimo de agilizar los procesos de seguimiento e identificación de posibles problemas.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.4 Paredes y Divisiones
Las paredes del Centro de Informática, deben extenderse desde el suelo hasta el cielo raso, con una altura mínima de 2.6 metros.	
Las paredes deben ser lo suficientemente rígidas de tal manera que soporten los equipos y dispositivos que se coloque en el área de cómputo.	
Las paredes deben ser de material incombustible y antiestático, exentas de materiales que expidan polvo.	
La pintura de las paredes debe ser pintura de agua, en colores claros y mate, que no forcé, ni cansen la vista de los funcionarios.	
Las paredes del Centro de Informática, deben estar perfectamente selladas, exentas de fisuras o resquebrajamientos.	
Las paredes deben estar libres de humedades, el Centro de Informática no debe esta en zonas que tengan tuberías de agua, canales o desagües.	
Se recomienda realizar revisiones por lo menos dos veces al año, para verificar el estado de las paredes y realizar el mantenimiento correspondiente.	
Los sitios de trabajo de los funcionarios y el mobiliario del Centro de Informática, deben ser de material incombustible y antiestático.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.5 Piso y Cielo Raso
El piso del Centro de Informática, debe ser construido en placa de concreto.	
El piso debe ser capaz de soportar una carga de 2.4 kPa	
El enchape del piso debe ser incombustible, antiestático y antideslizante. No debe utilizarse alfombra.	
La altura mínima del cielo raso medida a partir del piso es de 2.6 metros.	
El cielo raso debe construirse en placa de concreto, no se debe hacer uso de materiales combustibles o que expidan polvo.	
No deben existir dentro del Centro de Informática cielos falsos.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.6 Puertas
Para la puerta de acceso del Centro de Informática, se establece como mínimo 91 centímetros de ancho y 2 metros de alto.	
La puerta de acceso al Centro de Informática debe ser de apertura completa, abrir hacia afuera o de lado a lado y no debe tener postes centrales.	
Las puertas del Centro de Informática deben ubicarse de tal manera que abran a ras del piso.	
Las puertas y sus recibidores deben ser en metal y resistentes a accesos no autorizados.	
La puerta de acceso al área pública debe tener como mínimo una chapa de seguridad.	
Las puertas de acceso a las áreas limitadas y restringidas deben estar dotadas de mecanismos electrónicos que controlen el acceso de personal autorizado y su registro, tales como lectura por banda magnética o sistemas biométricos.	
Las llaves de la puerta de acceso al área pública del Centro de Informática, deben ser portadas por el Director y la secretaria de esta dependencia o por personal autorizado del Centro de Informática. No deben tener copias de las llaves, funcionarios no autorizados.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones Físicas
Elemento:	1.1.7 Ventanas
El área limitada y restringida de Centro de Informática no debe tener ventanas hacia el exterior del edificio.	
El área restringida no debe tener ventanas hacia el interior del edificio.	
De existir ventanas al interior del edificio en el área limitada deben estar protegidas por estructuras metálicas.	
De existir ventanas en el área pública deben estar protegidas por estructuras metálicas.	
La estructura metálica que protegen las ventanas, debe ser de tipo malla, sin que sus espacios excedan los 25 cm^2.	
Los soportes de las estructuras metálicas que protegen las ventanas, deben estar incrustadas dentro de las paredes.	
El anclaje de la estructura metálica debe resistir la presión de un gato mecánico de 500kg fuerza en el punto de aplicación.	
Los vidrios de las ventanas deben ser de seguridad.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.1 Construcción de Instalaciones físicas
Elemento:	1.1.8 Iluminación
Se debe proporcionar un mínimo equivalente a 540 lux medidos a un metro del piso terminado.	
La iluminación debe estar ubicada a un mínimo de 2,6 m del piso terminado.	
Las paredes deben estar pintadas de un color claro para mejorar la iluminación.	
El Centro de Informática debe mantener luz de color blanco.	
Se evitará la llegada directa del sol sobre los equipos y pantallas.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.2 Control de Ambiente.
Elemento:	1.2.1 Temperatura
El Centro de Informática debe mantener un control permanente de las condiciones ambientales.	
El Centro de Informática debe contar con termómetros permanentes que controlen los niveles de temperatura y que alerten en caso de registrar niveles fuera de los permitidos.	
El Centro de Informática debe mantener una temperatura constante de por lo menos 18ºC y 24ºC (grados centígrados).	
El cuarto de máquinas no debe exceder los niveles de temperatura sugeridos por los fabricantes de los equipos o dispositivos.	
El Centro de Informática debe contar con sistema de aire acondicionado para estabilizar el nivel de temperatura en el cuarto de máquinas.	
El Centro de Informática debe tener un adecuado sistema de ventilación.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.2 Control de Ambiente.
Elemento:	1.2.2 Humedad
La humedad relativa del Centro de Informática debe mantenerse dentro de los valores del 30% a 50 %.	
El cuarto de máquinas no debe exceder los niveles de humedad que exigen los fabricantes de los equipos o dispositivos.	
El Centro de Informática debe contar con sensores permanentes que controlen los niveles de humedad y que alerten en caso de registrar niveles fuera de los permitidos.	
El Centro de Informática debe contar con un sistema de calefacción para estabilizar los niveles de humedad.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.1 Incendios
Extintores	
Es responsabilidad de la Oficina de Servicios Generales, equipar al Centro de Informática y al edificio de extintores, de igual manera será responsable del mantenimiento y recarga de los mismos.	
Para el control, mantenimiento y recarga de los extintores, se asignará a personal capacitado que tengan a su alcance la maquinaría, herramientas y material de recarga adecuado.	
En el edificio donde se localiza el Centro de Informática se dispondrán extintores tipo ABC de 5 kg en cada piso, distribuidos en distancias no superiores a 15 m de recorrido horizontal, en cualquier dirección de acceso libre, o deben disponerse de acuerdo con el número de oficinas, mínimo un extintor por cada tres oficinas.	
El Centro de Informática será dotado con un extintor de CO2 de 5kg .	
Una vez realizada la dotación de extintores se realizará una planilla que indique los tipos y capacidades de los equipos instalados y su ubicación.	
Los extintores deben emplazarse en sitios de fácil acceso, que no estén obstruidos por objetos y que estén debidamente identificados y señalizados.	
Se debe prohibir estrictamente el uso de veladoras, cirios o lámparas de combustible dentro de las instalaciones.	
No se debe fumar dentro del área de cómputo.	
Después de la utilización de los extintores deben ser recargados y revisados. Se debe realizar revisiones periódicas para verificar el estado del extintor, carga y funcionamiento.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.1 Incendios
El personal del Centro de Informática debe ser capacitado en el manejo de equipos de seguridad y prevención de desastres por personal altamente calificado y que pueda certificar su conocimiento.	
Alarmas	
El Centro de Informática debe estar dotado de detectores de humo, alarmas contra incendios, perfectamente audibles, que alerten al personal del Centro de Informática y vigilancia, cuando haya presencia de fuego.	
Se debe realizar prueba de funcionamiento de las alarmas de manera periódica, informando previamente a los usuarios de la alarma de prueba.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.2 Inundaciones
No deben ubicarse equipos a nivel del suelo.	
Los niveles para el drenaje de agua, deben disponerse de tal manera que el nivel del edificio desemboque en los niveles de la parte externa de la edificación.	
El Centro de Informática debe ubicarse en un área distante de tuberías de agua, desagües, hidrates, grifos o aspersores.	
La Universidad de Nariño debe contar con motobombas, dispuestas para el uso exclusivo en casos de inundación.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.3 Terremotos
La construcción del edifico donde se ubica el Centro de Informática, debe cumplir con las Normas de Sismo Resistencia NSR-98.	
El personal del Centro de Informática debe estar capacitado en procedimientos de evacuación.	
No debe ubicarse equipos en superficies elevadas, ni cerca de las ventanas.	
No se debe situar objetos pesados en superficies altas cercanas a los equipos.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.4 Sabotaje
En caso de una toma del Bloque Administrativo, el Centro de Informática debe asegurar la puerta de las áreas limitada, restringida y pública, para evitar accesos indebidos a esta dependencia.	
Cerrar las sesiones de usuarios que estén activas.	
Apagar las estaciones de trabajo de los funcionarios que tienen acceso al servidor.	
Bloquear el acceso al computador mediante la configuración de clave de acceso al encendido de la maquina.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.3 Seguridad Frente a Desastres
Elemento:	1.3.5 Emergencias
En el Centro de Informática debe existir una cartelera en el que se encuentren los teléfonos de emergencia como: Policía Nacional, Bomberos, Defensa Civil, ambulancias, EPS – ARP.	
La Universidad de Nariño debe establecer un plan de actualización constante en el manejo de equipos de seguridad y prevención de desastres, al cual deben estar vinculados los funcionarios del Centro de Informática.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.4 Control de Acceso a las instalaciones.
Elemento:	1.4.1 Control de Acceso a Funcionarios del Centro de Informática
Los funcionarios del Centro de Informática deben portar un carné de forma visible que los identifique como funcionarios de ésta dependencia.	
El carné de identificación de los empleados del Centro de Informática es personal e intransferible, debe ser de un color que los distinga a simple vista de los empleados de otras dependencias y del personal visitante	
El carné contendrá fotografía, nombre del funcionario de manera legible, número del documento de identificación, dependencia y cargo que desempeña.	
Para el acceso al área pública no debe existir ningún tipo de restricción para empleados de la Universidad o personas ajenas a la institución.	
El ingreso a las áreas de acceso limitado, se establecerá de manera escrita especificando las funciones y responsabilidades de cada empleado autorizado para el acceso a esta área.	
El ingreso al área de acceso limitado debe realizarse a partir del área pública del Centro de Informática, no se debe acceder de una parte externa a las instalaciones.	
El acceso al área restringida, se establece únicamente para personal autorizado, que por razones específicas de trabajo puedan acceder a estos sitios y a los elementos que aquí se encuentren.	
Las áreas de acceso limitado y las áreas de acceso restringido deben permanecer cerradas, aún cuando se encuentre personal autorizado trabajando dentro de ella.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.4 Control de Acceso a las instalaciones.
Elemento:	1.4.1 Control de Acceso a Funcionarios del Centro de Informática.
Mantener por escrito una lista actualizada que detalle el personal autorizado para ingresar al Centro de Informática.	
Las llaves de la puerta de acceso al área publica del Centro de Informática, deben ser portadas por el Director y la secretaria de esta dependencia o por personal autorizado del Centro de Informática. No den tener copia de las llaves, funcionarios no autorizados.	
El personal de vigilancia debe tener claramente identificado al personal que trabaja en la dependencia del Centro de Informática.	
Es deber del Director del Centro de Informática informar de manera inmediata al personal encargado de vigilancia y de acceso de esta dependencia, si un funcionario deja de trabajar en esta dependencia.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.4 Control de Acceso a las instalaciones.
Elemento:	1.4.2 Control de Ingreso y Salida de Visitas
Las visitas del personal ajeno al Centro de Informática se identificarán con un carné que señale la función de visitante y de color correspondiente a la dependencia que visita.	
El personal de vigilancia de la Universidad de Nariño ubicado a la entrada de la institución, será el encargado de asignar éste carné, a cambio de un documento de identificación de la persona que ingresa.	
El documento de identificación del visitante se devolverá a la salida cuando entregue el carné que así lo distinguía.	
El acceso a las instalaciones del Centro de Informática por parte de personal ajeno a la dependencia, debe ser autorizado de manera escrita por el Director del Centro de Informática, de manera que la permanencia de estas personas dentro de las instalaciones de la dependencia estará bajo su responsabilidad.	
En el área de acceso público, habrá una sala o zona destinada para recibo de visitas con fines laborales, a los funcionarios del Centro de Informática, con el propósito que estas personas no ingresen a las instalaciones y sean atendidas allí.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.4 Control de Acceso a las instalaciones.
Elemento:	1.4.3 Control de Ingreso y Salida de Vehículos
Los vehículos que ingresen a la Universidad de Nariño deben tener de manera visible la calcomanía asignada por la Universidad. Es responsabilidad del vigilante de la entrada, el cumplimiento de esta norma, para el control de acceso de vehículos a las instalaciones de la Universidad de Nariño.	
Los vehículos que ingresen a la Universidad, serán revisados según los lineamientos de seguridad establecidos para la revisión de vehículos, verificando que en su interior no trasporten elementos explosivos.	
Si el vigilante encuentra un vehículo sospechoso debe pedir refuerzo al personal de vigilancia para impedir el ingreso del vehículo y el abandono de la persona que lo conduce y dar de inmediato informe a las autoridades.	
El interior de los vehículos también se examinará con el fin de verificar si ingresan computadores o cualquier otro tipo de equipos de computo a la Universidad, siendo el caso afirmativo el vigilante registrará el ingreso de estos equipos en una planilla anotando el nombre de la persona que ingresa, número del documento de identificación y las características del equipo que ingresa considerando nombre, cantidad, marca y numero de serie.	
Realizada la revisión correspondiente de los vehículos, el personal que ingrese a bordo de el, debe portar el carné que lo identifique como personal laborante de la Universidad, o si se trata de estudiantes deben presentar su carne que los distinga como tal, en las dos situaciones se debe verificar que el carné si corresponde a la persona que lo porta.	
Para la salida de equipos el vigilante debe verificar que el equipo que sale de la Universidad corresponde a las características señaladas en la planilla.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.4 Control de Acceso a las instalaciones.
Elemento:	1.4.4 Vigilancia
El Centro de Informática debe estar equipado con un sistema detector de intrusos, que permita detectar accesos de personal no autorizado, en horas no laborales.	
El sistema detector de intrusos, debe ser de tipo audible, y debe activarse en el momento o pocos minutos después de detectar la intrusión.	
Todo sistema de seguridad detector de intrusos, debe estar apoyado por una fuerza de reacción que atienda en el sitio que esta siendo o ya ha sido violado por el delincuente.	
Se debe verificar el funcionamiento del sistema de seguridad detector de intrusos de manera periódica.	
Las áreas de acceso limitado y restringido deben estar controladas por un Circuito Cerrado de Televisión CCTV, que realice grabaciones permanentes y se revisen con periodicidad.	
El Centro de Informática debe contar con vigilancia permanente, las 24 horas del día.	
Ubicar el personal de vigilancia del área perimetral, de manera que tengan una visibilidad máxima de cincuenta metros a la redonda.	
Debe existir un supervisor o persona encargada, que controle el desempeño en las rondas y puesto de vigilancia.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.5 Seguridad Equipos de Cómputo
Elemento:	1.5.1 Registro
Los equipos deben etiquetarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.	
Se debe mantener una bitácora de cada uno de los computadores que se tienen en el Centro de Informática, este documento debe especificar, marca del equipo, características técnicas, procesador, memoria, disco duro, placa base, dispositivos adicionales.	
Se debe mantener un registro de cada computador estableciendo que tipo de software tiene instalado, que tipo de licenciamiento, vigencia de la licencia, ubicación de las licencias y ubicación de los medios.	
En el Centro de Informática se debe mantener un registro actualizado de la ubicación de los equipos de cómputo.	
La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Director.	
Los equipos del Centro de Informática no pueden moverse ni ser trasladados, sin previa autorización escrita emanada por el Director.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.5 Seguridad Equipos de Cómputo
Elemento:	1.5.2 Mantenimiento
El Centro de Informática debe mantener un registro de los mantenimientos preventivos realizados a los equipos en donde se especifique: identificación del equipo, actividades de mantenimiento realizadas, novedades encontradas, responsable del mantenimiento, fecha y hora del mantenimiento.	
Se debe realizar plan de mantenimiento preventivo periódico, a los equipos de cómputo y dispositivos de red, por lo menos, una vez al año y registrarlo en la planilla de mantenimientos.	
En el Centro de Informática se debe mantener un registro de los mantenimientos correctivos que tienen los equipos que tiene a cargo.	
El registro de mantenimientos correctivos debe especificar serial de la máquina, ubicación, nombre del funcionario a cargo del equipo, novedades encontradas, diagnóstico del problema señalando posibles causas y firma de la persona que realiza el mantenimiento.	
El personal encargado del aseo del Centro de Informática debe estar capacitado para la realizar la limpieza correspondiente a los sitios donde se ubican equipos, servidores y cableado.	
El Centro de Informática debe recibir aseo diariamente, utilizando elementos que no produzcan polvo.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.6 Copias de Respaldo (Backups)
Elemento:	1.6 Copias de Respaldo (Backups)
El administrador de Sistema debe realizar un cronograma, especificando fecha y hora en que se realizaran copias de seguridad.	
Debe existir un documento que señale por escrito el procedimiento para realizar copias de seguridad.	
Antes de realizar la copia se debe verificar el buen estado del medio.	
Se debe mantener un registro de la realización de copias de seguridad, que indique: Medio, sistema respaldado, responsable de la copia, fecha y hora en que fue realizada.	
Las copias de seguridad deben almacenarse en medios magnéticos etiquetados con la siguiente información: Sistema respaldado, fecha y hora del respaldo.	
Las copias de seguridad deben almacenarse encriptadas.	
Las copias de seguridad deben almacenarse en un área restringida, organizadas cronológicamente, en gabinetes con llave.	
Se deben mantener tres copias de seguridad ubicadas de la siguiente manera: -En el Centro de Informática. -En un lugar fuera del edificio donde se localiza el Centro de Informática, dentro de la Universidad de Nariño. -Fuera de la Universidad, en un lugar seguro de acceso restringido.	
Debe existir un procedimiento escrito para restauración de copias de respaldo.	
La restauración de copias de seguridad se realizará bajo autorización escrita del Director del Centro de Informática.	

1. SEGURIDAD FÍSICA	
Aspecto:	1.6 Copias de Respaldo (Backups)
Elemento:	1.6 Copias de Respaldo (Backups)
Debe existir un registro que indique fecha, hora y persona responsable de restauración de copias de seguridad.	

2. SEGURIDAD INSTALACIONES ELÉCTRICAS	
Aspecto:	2.1 Redes Eléctricas
Elemento:	2.1.1 Puesta a Tierra
El Centro de Informática debe contar con una instalación de puesta a tierra acorde con la carga de equipos.	
La puesta a tierra del Centro de Informática se hará de forma que no se alteren las condiciones de puesta a tierra de la red de la empresa eléctrica	
La medida entre neutro y tierra no debe ser mayor a 0,6 voltios.	
Los computadores, impresoras y equipos de comunicaciones deben utilizar la misma tierra.	
El circuito eléctrico del edificio donde se encuentra el Centro de Informática, debe estar protegido con pararrayos.	

2. SEGURIDAD INSTALACIONES ELÉCTRICAS	
Aspecto:	2.1 Redes Eléctricas
Elemento:	2.1.2 Circuito Eléctrico
Las instalaciones eléctricas del Centro de Informática deberán cumplir con las normas eléctricas establecidas por el REGLAMENTO TÉCNICO DE INSTALACIONES ELÉCTRICAS – RETIE.	
El Centro de Informática debe tener un circuito eléctrico independiente al utilizado por las demás dependencias del edificio.	
Los circuitos eléctricos para el Centro de Informática deben garantizar tres líneas de alimentación: Fase, Neutro y Tierra.	
El circuito eléctrico debe estar balanceado y debidamente aterrizado de acuerdo a la carga de equipos que soportará y pensando en la escalabilidad.	
Se debe colocar entre los equipos y la red de energía pública elementos de barrera como: reguladores o acondicionadores de voltaje y supresores de equipos de voltaje, acordes a la capacidad de carga que deben soportar.	
Los elementos de barrera deben mantener un voltaje promedio 110 – 115 Voltios.	
A la salida de los elementos de barrera, se debe instalar un tablero auxiliar con “barras aisladas” para neutros y tierras y para minimizar la caída de tensión en los conductores, no se debe manejar más de 10 o 15 Amperios en cada circuito, ni compartir cables entre circuitos diferentes.	
El color de cable para neutros debe ser blanco o gris, la tierra color verde (continuo o con rayas amarillas) y los vivos negros o de cualquier otro color diferente.	

2. SEGURIDAD INSTALACIONES ELÉCTRICAS	
Aspecto:	2.1 Redes Eléctricas
Elemento:	2.1.2 Circuito Eléctrico
La conexión de los toma eléctricos se debe realizar de manera que la ranura pequeña reciba la fase, la ranura grande el neutro y la redonda para conectar el cable de conexión a tierra.	
La Resistencia del cableado eléctrico, no puede exceder 9.38 Ohm/100m, y tampoco debe haber diferencias de más de 5% entre los cables del mismo par.	
La Capacitancia del cableado eléctrico no debe exceder 6.6 nF a 1 khz.	
La Impedancia del cableado eléctrico como característica 100 +/- 15%.	

2. SEGURIDAD INSTALACIONES ELÉCTRICAS	
Aspecto:	2.1 Redes Eléctricas
Elemento:	2.1.3 Mantenimiento
El proceso de mantenimiento debe contemplar controles periódicos, observando en detalle la instalación, su estado de limpieza, si hay presencia de óxido, humedad, quemaduras, ennegrecimiento, roturas, puntos calientes, tornillos flojos, lámparas quemadas, reactancias, capacitores, tomacorrientes dañados o cables sueltos.	
El Centro de Informática debe llevar un registro de los resultados de la inspección, las fallas importantes y las acciones que se ejecuten a la red eléctrica.	
Las acciones de corrección y arreglo se deben planear y ejecutar en forma conveniente, de acuerdo a la importancia, uso de la instalación y de la urgencia.	
Se debe revisar periódicamente el correcto funcionamiento de los equipos de respaldo eléctrico.	
Los equipos de respaldo eléctrico deben recibir mantenimiento periódico, el cual será registrado en un documento que especifique: equipo, fecha del mantenimiento, estado del funcionamiento y actividades realizadas.	
Se debe garantizar que la capacidad de la puesta a tierra no sea excedida, en la carga que esta instalada.	
Se debe realizar revisiones constantes a la puesta a tierra del Centro del Informática garantizado que su voltaje no exceda los 0.6 voltios.	
Se debe mantener húmedo el terreno donde se ubica la puesta a tierra.	

2. SEGURIDAD INSTALACIONES ELÉCTRICAS	
Aspecto:	2.2 Respaldo Eléctrico
Elemento:	2.2.1 UPS y Planta Eléctrica
El Centro de Informática debe contar con un sistema de respaldo de planta eléctrica el cual se activará en caso de caída de energía.	
La planta eléctrica debe garantizar el funcionamiento de la totalidad de los equipos que trabajan en el Centro de Informática.	
Los sistemas de corriente ininterrumpida deben estar dispuestos para los equipos de cómputo como computadores, servidores y equipos de comunicación.	
La capacidad de la UPS debe ser acorde con la cantidad de equipos a los que genera respaldo dejando un margen de por lo menos 20% de carga libre.	
Los circuitos deben ser regulados a través de estabilizadores, protegidos con puesta a tierra y soportados por un sistema de corriente ininterrumpida (UPS) de por lo menos 20 minutos para poder realizar un correcto apagado de las máquinas en caso de ser necesario o tiempo para la activación la planta eléctrica.	
Las UPS utilizadas deben ser administrables y permitir programar actividades en caso de caída de energía.	
Se deben revisar periódicamente el correcto funcionamiento del los equipos de respaldo eléctrico.	
Los equipos de respaldo eléctrico deben recibir mantenimiento periódico, el cual será registrado en un documento que especifique: equipo, fecha del mantenimiento, estado del funcionamiento y actividades realizadas.	

3.REDES DE DATOS	
Aspecto:	3.1 Red Física
Elemento:	3.1.1 Dispositivos y Conexión
La implementación de cableado debe estar sujeta al estándar ANSI/TIA/EIA-568-A.	
Las vías y espacios de comunicaciones debe estar sujeta al estándar ANSI/TIA/EIA-569.	
Para la administración de infraestructura, codificaciones de colores, etiquetado, y documentación de comunicaciones debe estar sujeta al estándar ANSI/TIA/EIA-606.	
La conexión de redes sobre cable coaxial, par trenzado y medios de fibra óptica deben estar sujetos al estándar IEEE ISO 8802-3.	
Los esquemas de red basados en métodos de implementación por tecnología Token Bus se deben ajustar al estándar IEEE ISO 8802-4.	
Los protocolos de acceso, cableado e interfase para una LAN Token Ring se especifican bajo el estándar IEEE ISO 8802-5.	
Las redes de área metropolitana MAN, se deben ajustar al estándar IEEE ISO 8802-6.	
Los parámetros para la definición de anchos de banda deben estar sujetos al estándar IEEE ISO 8802-7.	
La implementación de redes a través de fibra óptica debe estar sujeta al estándar IEEE ISO 8802-8.	
Las Redes Integradas de Datos y Voz a través de nodos definidos en teléfonos, computadoras y codificadores/decodificadores de vídeo (codecs) deben estar sujetos al estándar IEEE ISO 8802-9.	
Los modelos de trabajo en seguridad en redes de datos deben estar guiados por el estándar IEEE ISO 8802-10.	
La implementación de redes de tipo inalámbrico debe estar sujeta al estándar IEEE ISO 8802-11.	

3. REDES DE DATOS	
Aspecto:	3.1 Red Física
Elemento:	3.1.1 Dispositivos y Conexión
Para la protección de redes de tipo inalámbrico, el administrador de la red de datos debe ajustarse al estándar 802.11 que define el equivalente en conexión con cable, la seguridad de redes inalámbricas (WEP, Wire Equivalent Privacy).	
Los puntos de acceso adquiridos para redes inalámbricas deben permitir autenticación por dirección MAC, debe ser administrable por interfase Web y manejado por claves de acceso.	
Se deben realizar monitoreos de las redes inalámbricas para evaluar su estado y determinar posibles debilidades en el modelo de seguridad.	
Se debe garantizar que no se transmita el SSID (identificador de conjunto de servicios).	
Se deben ubicar los puntos de acceso, de modo que su alcance desde el exterior del edificio se encuentre limitado tanto como sea posible.	
Los dispositivos de conexión deben estar ubicados en cajas de seguridad con llave.	
Los racks que contengan el cableado del la red de datos deben estar organizados mediante regletas, en los cuales se relacione los puntos de red que se manejan mediante un diagrama ubicado en el mismo en un lugar no visible.	
los puntos de red deben estar debidamente etiquetados, y se debe mantener un control del los puntos utilizados y los que se encuentran fuera de servicio, los puntos fuera de servicio deben estar desconectados del los dispositivos de comunicación como hub, routers, switch.	
Los diferentes elementos de la red de datos como cables, terminales, jacks, face place, canaleta, tubería deben: Ser de material auto consumible en caso de incendio. Deben ser instalados de manera independiente a otro tipo de redes como las eléctricas o de voz. Los materiales deben estar certificados por estándares internacionales como el de la IEEE.	

3. REDES DE DATOS	
Aspecto:	3.1 Red Física
Elemento:	3.1.1 Dispositivos y Conexión
El cableado debe estar protegido a través de canaleta, tubos, tubo corrugado, no debe por ningún motivo estar suelto en ninguna sección del tirado.	

3. REDES DE DATOS	
Aspecto:	3.1 Red Física
Elemento:	3.1.2 Diseño

El Centro de Informática mantendrá un diagrama de la red de datos que deberá vincular información correspondiente a:

- Tipos y números de los sistemas en la red.
- Sistemas Operativos y versiones.
- Topologías de red
- Puntos de acceso a Internet.
- Usos de Internet.
- Tipo, número y versiones de los muros de fuego.
- Puntos de acceso por marcación telefónica
- Puntos de acceso inalámbrico.
- Tipo del acceso remoto.
- Topología de la red amplia
- Puntos de acceso a sitios remotos
- Puntos de acceso a otras organizaciones
- Ubicaciones de los servidores de Web, FTP, Gateways.
- Protocolos utilizados
- Responsable del control de la red.

El Centro de Informática debe mantener un documento actualizado que identifique los mecanismos de protecciones que contiene la red de datos, vinculando la siguiente información.

- Listas de control de acceso al enrutador.
- Reglas de los muros de fuego.
- Mecanismos de autenticación o validaciones utilizados para el acceso remoto.
- Mecanismos de protección en puntos de acceso hacia otras organizaciones.
- Mecanismos de encriptación utilizados para proteger las computadoras portátiles.
- Sistemas antivirus instalados en los servidores y estaciones de trabajo.
- Configuraciones de seguridad en los servidores.

El administrador de la red de datos debe mantener un registro actualizado de la información y dispositivos compartidos en la red.

El Comité de Sistemas debe tomar como punto de partida el estándar ISO/IEC17799 information Tecnology – code of practice for information segurity, para la implementación de sistemas de seguridad.

3. REDES DE DATOS	
Aspecto:	3.1 Física
Elemento:	3.1.3 Mantenimiento
Los sistemas de cableado deben recibir revisión dos veces al año, en la que se determine el estado de la red, estado de calidad de transmisión, velocidad, pérdidas de paquetes.	
Se debe realizar una revisión periódica de los puntos de red como cajas, jacks, Patch Cords.	
Se debe realizar un mantenimiento periódico de los dispositivos de conexión de la red.	
Los dispositivos de conexión deben estar ubicados en lugares que permitan mantener las temperaturas sugeridas por los productores, y ubicarse en lugares de bajo tráfico de personal, protegidos por rack y asegurados bajo llave.	
Los Racks deben recibir aseo por personal especializado de manera periódica.	

3. REDES DE DATOS	
Aspecto:	3.2 Servicios
Elemento:	3.2.1 Recursos De Red
Cada funcionario es responsable de proteger la información confidencial que llegue a sus manos.	
Es responsabilidad de Centro de Informática la implementación de mecanismos de seguridad que garanticen la integridad, confidencialidad, disponibilidad de la información.	
La información confidencial debe ser protegida por reglamentación o leyes internas.	
El administrador de la red de datos debe mantener un control de los recursos compartidos en la red.	
En caso de que los usuarios necesiten compartir datos residentes en un computador, deberán usar correo electrónico y/o Directorios públicos que sean habilitados por el Centro de Informática.	
Los servicios de News, chat, Real Audio, Netmeeting, mensajeria instantánea, descarga de música y programas, deben estar bloqueados. Si algún usuario necesita utilizar alguno de estos servicios por razones de trabajo, se debe realizar una solicitud por escrito, especificando el servicio, la hora y fecha exactas en que lo va a utilizar con su respectiva justificación y visto bueno del Jefe de la Dependencia. El servicio será habilitado temporalmente y específicamente para el usuario autorizado.	
Cuando un funcionario recibe una nueva cuenta de usuario, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.	
La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrito y ser debidamente aprobada.	
No debe concederse una cuenta a personas que no sean trabajadores de la Universidad de Nariño a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente en un lapso de 30 días o inmediatamente termine su trabajo.	

3. REDES DE DATOS	
Aspecto:	3.2 Servicios
Elemento:	3.2.1 Recursos De Red
Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.	
La información que viaja a través de la red de datos debe estar encriptada mediante algún algoritmo de encriptación que esta establecido por la institución	
Cuando un trabajador es despedido o renuncia a la Universidad, debe desactivarse su cuenta antes de que deje el cargo.	
Si no ha habido actividad en una terminal, PC o estación de trabajo durante cierto periodo de tiempo, el sistema debe automáticamente bloquear la pantalla y suspender la sesión. El periodo recomendado de tiempo es de diez minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique nuevamente.	
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 Universidad, pudiendo ser causal de despido.	
Los servidores de red y los equipos de comunicación deben estar ubicados en lugares apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos lugares y a los cuartos de cableado a personas no autorizadas.	

3. REDES DE DATOS	
Aspecto:	3.2 Servicios
Elemento:	3.2.1 Recursos De Red
No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Director del Centro de Informática lo determinen necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo.	
Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.	
Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" o “su” para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.	
Toda cuenta queda automáticamente suspendida después de 30 días de inactividad.	
Se debe contar con un servidor de autenticación que permita reconocer los usuarios que hacen parte de la red de datos.	

3. REDES DE DATOS	
Aspecto:	3.2 Servicios
Elemento:	3.2.2 Internet
Los servicios de Internet deben estar restringidos al uso apropiado de los mismos en actividades académicas o laborales de la Universidad.	
Los servidores de correo electrónico deben estar configurados de tal forma que permitan realizar la identificación de posibles virus en archivos adjuntos.	
Se deben restringir los servicios de mensajera instantánea por Internet, descarga de música, emisoras y canales de televisión.	
Se debe especificar claramente los servicios de Internet que serán prestados y configurar el muro de fuego para que autorice el trafico de paquetes únicamente de esos servicios.	
La descarga de programas por Internet debe estar restringida, este proceso de ser necesario será realizado por personal especializado que determinara que tipo de programa, licenciamiento y la viabilidad e la instalación del mismo en computadores de la Universidad.	
No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.	
Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.	
No emplear los máximos privilegios en tareas para las que no sean estrictamente necesarios.	
No se debe confiar en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus	
Configurar el sistema para que muestre las extensiones de todos los archivos.	
De ninguna manera se debe ejecutar ningún archivo con doble extensión.	

3. REDES DE DATOS	
Aspecto:	3.2 Servicios
Elemento:	3.2.2 Internet
No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos , tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.	
Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.	
Se debe borrar constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.	
Los correos electrónicos debe registrar una firma digital que identifique la persona que envía el mensaje.	

3. REDES DE DATOS	
Aspecto:	3.3 Control Lógico
Elemento:	3.3.1 Servidores
Debe existir un plan de capacitación continuo para los funcionarios de la Universidad de Nariño en la concientización sobre los temas relacionados en seguridad.	
Los servidores deben configurarse de forma que permitan realizar revisión de log´s del servidor, frente a los accesos al sistemas, es decir de conexiones o entradas al sistemas.	
Los servidores deben configurarse de forma que permitan realizar revisión de log´s, frente a los logouts, es decir de salidas o desconexiones del sistemas.	
Los servidores deben configurarse de forma que permitan realizar revisión de log´s de acceso fallido al sistema, servicios o archivos.	
Los servidores deben configurarse de forma que permitan realizar revisión de log´s de accesos remotos con o sin éxito.	
Se debe mantener un log de acciones privilegiadas realizadas por los administradores.	
Los servidores serán instalados en áreas de tipo restringido.	
Los servidores se deben configurar de tal manera que los archivos de arranque ejecuten únicamente los servicios para los cuales esta dispuesto el servidor.	
Los servicios que no sean propios de cada servidor, se ejecutaran de forma manual, con autorización el administrador del sistema.	
Los servidores deben estar configurados para garantizar un número mínimo de caracteres para las contraseñas y un tiempo mínimo de caducidad.	
El servidor debe garantizar los privilegios iniciales que deben contener los archivos que se generen, los cuales deben corresponder a la siguiente configuración: Propietario: lectura, escritura y ejecución. Grupo de trabajo: No lectura, No escritura y No ejecución. Otros usuarios: No lectura, No escritura y No ejecución.	

3. REDES DE DATOS	
Aspecto:	3.3 Control Lógico
Elemento:	3.3.1 Servidores
Se debe mantener un control sobre las cuentas de usuario que se manejan en el servidor y deshabilitar las que se encuentren fuera de uso.	
El servidor debe restringir a los usuarios, que no sean tipo administrador, el acceso a los archivos del sistema, la raíz principal del mismo y archivos de configuración.	

3. REDES DE DATOS	
Aspecto:	3.3 Control Lógico
Elemento:	3.3.3 Monitoreo
Para la prevención y detección de ataques se debe implementar sistemas de detección de intrusos (ISD).	
El Centro de Informática debe contar con herramientas para monitoreo y análisis de tráfico y control de accesos a Internet (herramientas IDS, administradores de URLs, firewalls)	

4. SEGURIDAD LÓGICA	
Aspecto:	4.1 Proyectos de Software
Elemento:	4.1.1 Planeación del Proyecto
La propuesta de desarrollo de software debe incluir los requerimientos de seguridad necesarios basado en un previo estudio que establezca las medidas de seguridad necesarias para el funcionamiento del sistema.	
Debe realizarse un estudio tecnológico y determinar si los recursos de seguridad actuales con que cuenta el Centro de Informática permiten que el desarrollo e implementación del software minimice la vulnerabilidad del sistema.	
Para los proyectos de desarrollo, se debe asignar un Auditor relacionado con el tema del desarrollo, que facilite la identificación de posibles falencias de seguridad que pueda presentar el sistema.	
En el desarrollo del software habrá participación de Auditores, que aseguren la implantación de controles y pistas de auditoría en la aplicación.	
Dentro de la estructura orgánica se establecerá el administrador de la seguridad para el desarrollo del proyecto. Este puede también ejecutar otras actividades dentro del plan de desarrollo.	
El Comité de Sistemas deberá poner en conocimiento las normas, políticas y requerimientos de seguridad al Director del proyecto.	
El Director del proyecto se encargara de establecer y definir procedimientos para el cumplimiento de las normas y políticas de seguridad que el proyecto haya determinado.	
El personal para el desarrollo debe tener una adecuada formación y estar motivado para la realización de su trabajo. Si participa personal externo en el desarrollo del proyecto, éste debe cumplir con los perfiles profesionales, de acuerdo a las funciones que va a realizar y los requerimientos de seguridad que el proyecto determine.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.1 Proyectos de Software
Elemento:	4.1.1 Planeación del Proyecto
El personal de otras áreas cuya participación sea relevante para el desarrollo del proyecto debe ser autorizado por escrito por el Director de la dependencia a la cual pertenezca.	
Haciendo uso de la información puesta a disposición, el Director del proyecto, enmarcará el desarrollo del mismo dentro de alguna de las metodologías propuestas por la Ingeniería de Software.	
El Comité de Sistemas y el Director del proyecto, deberán evaluar los riesgos ligados al mismo en especial cuando se trate de implementar nuevas tecnologías.	
El Director del proyecto velará por el cumplimiento de las etapas establecidas, según la metodología implantada para el desarrollo de software.	
Todas las etapas del desarrollo deben documentarse y cumplirse a cabalidad. No se debe iniciar una nueva etapa sin haber documentado, revisado y aceptado la etapa previa.	
Al finalizar el proyecto se debe revisar que la información sea completa y quede catalogada perfectamente, para garantizar la facilidad de acceso para revisiones posteriores.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.1 Proyectos de Software
Elemento:	4.1.2 Definición de Seguridad
En el levantamiento de la información, se debe tener en cuenta los procesos críticos en el manejo de la información, para determinar posibles problemas de seguridad y optimizar el sistema en este aspecto.	
Se deben describir los problemas de seguridad con los que cuenta el modelo de funcionamiento actual, y describir claramente los posibles controles de seguridad que se puedan establecer.	
Una vez que se conozca el sistema de seguridad actual y se hayan identificado los requerimientos de seguridad, se elaborará las especificaciones funcionales del sistema.	
El grupo de diseño debe plantear un modelo que especifique un panorama donde defina un esquema de seguridad que minimice el riesgo de posibles ataques internos o externos.	
El administrador de la seguridad en el desarrollo del proyecto revisará que en la etapa de diseño se contemplen controles y pistas de auditoría que permitan hacer auditable la aplicación.	
El Director o responsable del proyecto, revisará que las actividades realizadas en el diseño sean correctas, coherentes con la etapa previa de análisis, que se realicen de acuerdo a normas, estándares y con las técnicas adecuadas para minimizar los posibles riesgos de seguridad que afecten la integridad, confidencialidad y disponibilidad de la información.	
El diseño del modelo de seguridad del sistema debe garantizar el registro de las actividades que realicen los usuarios, contemplando los campos de identificación del usuario, hora y fecha de inicio, dato anterior, dato modificado y fecha y hora de salida.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.1 Proyectos de Software
Elemento:	4.1.2 Definición de Seguridad
El diseño del sistema debe ir acompañado de algoritmos de encriptación que permitan garantizar la seguridad de la información mediante un correcto cifrado.	
Se deben establecer los requerimientos de hardware y software compatible con DBMS y Sistemas Operativos.	
El Director del proyecto debe proporcionar lineamientos en situaciones normales e imprevistas del procesamiento de datos (como mantenimiento del sistema, acciones frente a interrupciones eléctricas o caídas de red de datos, restauración del sistema y recuperación del sistemas o información).	

4. SEGURIDAD LÓGICA	
Aspecto:	4.1 Proyectos de Software
Elemento:	4.1.3 Desarrollo de Software
El administrador de seguridad del proyecto debe garantizar que el código fuente este exento de líneas maliciosas, bombas lógicas, Caballos de Troya u otro tipo de código que afecten la integridad, confidencialidad y disponibilidad de la información.	
El administrador de seguridad del proyecto debe revisar la programación de los logs del sistema, garantizando que se ajusten a los diseños establecidos.	
La programación debe realizarse de acuerdo a los estándares establecidos, en la planeación del proyecto.	
Debe existir un documento que especifique el tipo de nombramiento para las variables, funciones, rutinas para lograr una programación unificada.	
El administrador de seguridad del proyecto debe revisar que se este cumpliendo en la codificación el nombramiento establecido.	
El código debe estar debidamente comentariado, definiendo variables y funciones.	
El Director del proyecto es el encargado de garantizar que se realice una adecuada administración de las versiones del software.	

4. SEGURIDAD LÓGICA	
Aspecto:	4. 2 Adquisición de Software
Elemento:	4.2.1 Compra de Software
Se debe contar con análisis de procesos de la institución de manera que refleje las necesidades, debilidades que tenga la institución y que justifiquen la compra de determinado software.	
Deben identificarse claramente las áreas responsables de la contratación, ejecución y cumplimiento del contrato desde la solicitud del usuario teniendo en cuenta los niveles de autorización establecidos, incluyendo revisiones de lo que se solicita y cubrimiento de garantías y servicios postventa.	
El software a adquirir, debe garantizar manejo de tablas de auditoría en que se registren todas las actividades que realice el usuario.	
El software debe contemplar algoritmos de encriptación de la información que permita garantizar la seguridad de la información mediante un correcto cifrado.	
Se debe especificar los requerimientos de hardware para los cuales el software logra su mayor eficiencia.	
Se debe contar con los manuales de operación del administrador y usuarios.	
Los manuales de operación deben proporcionar a los usuarios información sobre los procedimientos para el correcto manejo del software.	
Los manuales de operación para el administrador debe proporcionar los procedimientos a seguir en situaciones imprevistas como violación de claves, caídas de red.	
Los usuarios deben ser capacitados por la empresa prestadora de servicio para el manejo, administración y orientación en el manejo de la información.	

4. SEGURIDAD LÓGICA	
Aspecto:	4. 2 Adquisición de Software
Elemento:	4.2.1 Compra de Software
La empresa prestadora del servicio debe capacitar de manera especial para la administración del sistema en procesos críticos como mantenimiento, restauración de sistema, recuperación de datos.	
Se debe concientizar a los usuarios del sistema, de la importancia de mantener la privacidad de la información, usuarios y contraseñas.	
El licenciamiento debe especificar la propiedad del código fuente, librerías y ejecutable.	
Se debe especificar el tipo de software al cual pertenece, freeware, GNU, libre, comercial.	
La licencia debe especificar la vigencia de la misma para determinar tiempos de uso del software.	
Se debe especificar los alcances de las actualizaciones del software.	
El software debe especificar la seguridad de la información en la encriptación de los datos en el almacenamiento y acceso.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.2 Adquisición de Software
Elemento:	4.2.2 Outsourcing
Se debe contar con análisis de procesos de la institución de manera que refleje las necesidades, debilidades que tenga la institución y que justifiquen la sistematización de los procesos.	
Deben identificarse claramente las áreas responsables de la contratación, ejecución y cumplimiento del contrato desde la solicitud del usuario teniendo en cuenta los niveles de autorización establecidos, incluyendo revisiones de lo que se solicita y cubrimiento de garantías y servicios postventa.	
Al momento de la contratación el proveedor deberá disponer de certificados de existencia y representación legal, y tener una póliza de cumplimiento y de calidad de servicio, equivalente a un porcentaje del valor del contrato.	
Durante la vigencia del contrato el proveedor estará disponible para atender las necesidades previstas y no previstas en el plan de trabajo. De esta manera se asegura la disponibilidad permanente del personal, metodologías herramientas y asesoría técnica cada vez que se requiera.	
El proveedor debe comprometerse con la confidencialidad, integridad y consistencia de la información y seguridad de la misma.	
El proveedor realizará la configuración y estructuración de la seguridad física y lógica del sistema de la empresa o servicio que se este contratando.	
El proveedor debe especificar los procedimientos para la realización de copias de seguridad de la información en archivos planos.	
La empresa prestadora del servicio debe garantizar dejar copia de información en forma de archivos planos.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.1 Utilización de los Sistemas
Los sistemas de la Universidad de Nariño, serán accedidos exclusivamente por usuarios autorizados del sistema y únicamente para fines relacionados con la funcionalidad de los procesos que maneje la Universidad.	
Los usuarios de los sistemas de la Universidad de Nariño, deben abstenerse del uso de los mismos para propósitos personales.	
El uso de los sistemas para fines ajenos a los establecidos por la Universidad, deben ser previamente evaluados y autorizados mediante documento escrito por el Director del Centro de Informática.	
En caso de ser utilizados los sistemas de la Universidad, para propósitos ajenos a la institución sin previa autorización, este hecho se considerará como violación de los derechos de la Universidad y recaerá sobre él, sanciones correspondientes al abuso de confianza.	
El sistema debe emitir al usuario en la pantalla inicial, un mensaje que advierta sobre el uso exclusivo del sistema para fines de la Universidad.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.2 Identificación y Autenticación de Usuarios
Los usuarios de los sistemas que maneja el Centro de Informática de la Universidad de Nariño, deben acceder a ellos de forma individual, a través de un Nombre de Usuario y una Contraseña.	
Cuando un funcionario recibe una cuenta de usuario, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad y acepta sus responsabilidades con relación al uso de esa cuenta.	
Existirá un servidor de autenticaciones en el cual los usuarios se identificarán y posterior a este proceso, si se trata de un usuario autorizado, el servidor se encargará de autenticarlo a los demás sistemas a los cuales tenga acceso.	
El usuario y contraseña de acceso al sistema, es de uso personal e intransferible, no se debe suministrar a ninguna persona ni puede ser compartida. El acreedor del identificador se hace responsable de todas las actividades que se realicen con él.	
Cuando por razones de fuerza mayor deban ser suministradas las contraseñas, se debe cambiar la clave con la menor brevedad de tiempo posible y quedar registrada la contingencia en un acta donde se especifique las razones, hora y fecha desde y hasta cuando fue utilizada por otra persona. En estos casos la solicitud o determinación de la contingencia la debe autorizar un cargo superior.	
El número de intentos que se le permiten al usuario para ingresar la contraseña es de tres, después de los cuales se bloquea la terminal desde la cual se esta intentando realizar el ingreso. Debe procederse a investigación inmediata para saber si trata de errores del usuario o intentos de suplantación.	
Una vez que el usuario se haya identificado y autenticado en el sistema, si la máquina presenta inactividad durante un periodo de diez minutos, el sistema debe bloquear la pantalla y suspender la sesión. El usuario si desea volver a entrar, debe autenticarse nuevamente.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.2 Identificación y Autenticación de Usuarios
El Centro de Informática mantendrá una planilla designada como “Control de Usuarios”, que contendrá una lista de los usuarios habilitados en el sistema y sus privilegios, al igual que los usuarios que hayan sido dados de baja. Esta planilla debe permanecer archivada en una carpeta organizada cronológicamente y será de consulta para Controles administrativos de Auditoría.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.3 Control de Usuarios
Creación de Usuarios	
La creación de usuarios en el sistema, debe ser autorizada por el Director del Centro de Informática y será efectuada por el administrador del sistema principal	
Debe crearse un único súper-usuario de operación permanente, los demás funcionarios del Centro de Informática son usuarios con privilegios específicos de acuerdo a sus funciones.	
Existirá dentro del sistema un súper usuario de respaldo, del cual tendrá conocimiento exclusivo el Director del Centro de Informática, quien hará uso en caso que el administrador del sistema por alguna situación imprevista llegara a faltar, restableciendo así el control sobre el sistema, durante el tiempo en que el administrador del sistema se reintegre o remplace; quedando registro de todas las operaciones que esta persona realice.	
Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" o “su” para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.	
Pueden establecerse usuarios temporales durante un determinado periodo de tiempo, según la función del usuario lo requiera, al finalizar este periodo el usuario se eliminará del sistema.	
Toda creación de usuarios en el sistema, debe registrarse en la planilla de “Control de Usuarios”.	
Modificación de Usuarios	
La modificación de usuarios en el sistema, debe ser autorizada por el Director del Centro de Informática y será efectuada por el administrador del sistema principal.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.3 Control de Usuarios
Para poder modificar un Usuario este NO debe estar habilitado en ninguna Terminal.	
Si un funcionario cambia de cargo, deben modificarse sus privilegios de acuerdo a sus nuevas funciones.	
Toda modificación de usuarios en el sistema, debe registrarse en la planilla de "Control de Usuarios".	
Eliminación de Usuarios	
La eliminación de usuarios en el sistema, debe ser autorizada por el Director del Centro de Informática y será efectuada por el administrador del sistema principal.	
La eliminación de usuarios del sistema se realizará por razones de traslado o retiro definitivo del funcionario.	
Los usuarios establecidos temporalmente en el sistema deben eliminarse finalizado el periodo de actividad.	
Toda eliminación de usuarios en el sistema, debe registrarse en la planilla de "Control de Usuarios".	
Administración de Cuentas de Usuario	
La administración de las cuentas de usuario y los privilegios del sistema asignados a los usuarios, deben revisarse cada seis meses.	
Los usuarios deben tener dentro de las opciones del menú, la posibilidad de cambiar su contraseña, el sistema a su vez deberá registrar fecha y hora del último nombre de usuario.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.3 Control de Usuarios
Mensualmente el Director del Centro de Informática debe validar que todos los Usuarios creados en el sistema estén laborando. Los que ya han sido trasladados o retirados no deben figurar como Usuarios habilitados, si se trata de un cambio de cargo deben replantearse sus privilegios de usuario.	
Todos los recursos del sistema deben estar identificados y clasificados dentro de una jerarquía de acuerdo a niveles de seguridad, de tal modo que los usuarios puedan acceder a ellos según el nivel de autorización.	
En caso de que un funcionario deba realizar un retiro temporal por licencia u otro motivo autorizado por las directivas de la institución, el usuario deberá inhabilitarse por el administrador del sistema, durante el periodo de tiempo establecido.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.4 Especificaciones de Contraseña
La contraseña tendrá una longitud establecida dentro de un rango de seis (6) a ocho (8) caracteres.	
La contraseña no debe ser secuencial y debe mantener una combinación alfanumérica, compuesta por letras mayúsculas (A-Z), letras minúsculas (a-z) y dígitos (0-9).	
Los usuarios al establecer la contraseña en el sistema, deben evitar utilizar información que sea de fácil consecución por personas mal intencionadas, tal como números telefónicos, fechas de nacimiento, nombres de personas, nombres de mascotas o cualquier otro tipo de datos personales.	
La contraseña será establecida directamente por el usuario.	
Las contraseñas se almacenarán cifradas bien sea por procedimientos de encriptación desarrollados en el Centro de Informática o por mecanismos propios del sistema operativo o sistemas de Encriptamiento.	
La contraseña será de propiedad individual del usuario y será este el responsable de la protección del mismo evitando su divulgación.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.5 Vigencia de la Contraseña
Las contraseñas deben tener una vigencia de treinta (30) días.	
El sistema alertará con ocho (8) días de anticipación al vencimiento de la contraseña, emitiendo un mensaje al usuario, informando sobre la caducidad y sugiriendo cambio de contraseña en los 8 días siguientes.	
Si el usuario no atendió la petición de cambio de contraseña al primer aviso, el sistema seguirá emitiendo durante los siguientes siete días (7) el mensaje sugiriendo cambio de contraseña.	
Si el usuario cumplido los treinta (30) días de vigencia, no ha realizado el cambio de contraseña, el sistema no le permitirá ingresar hasta no establecer una nueva contraseña.	
Pasados los treinta (30) días, si el usuario no ha manifestado cambio de contraseña, el sistema lo dejará inactivo.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.6 Entrada y Transmisión de la Contraseña
La contraseña debe protegerse de manera que los caracteres no se impriman en la pantalla.	
La contraseña será encriptada en el momento de su ingreso y se transmitirá encriptada hasta el servidor que administre la autenticación.	
El servidor que realice la autenticación realizara la desencripción de las claves.	
Si el usuario sospecha que fue observado mientras digitaba su contraseña de acceso, debe de manera inmediata proceder a realizar un cambio de contraseña.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.3 Control de Acceso
Elemento:	4.3.7 Periodo de Autenticación
El número de intentos que se le permiten al usuario para ingresar la contraseña es de tres (3), después de los cuales se bloquea la terminal desde la cual se esta intentando realizar el ingreso. Debe procederse a investigación inmediata para saber si trata de errores del usuario o intentos de suplantación.	
Una vez que el usuario se haya identificado y autenticado en el sistema, si la máquina presenta inactividad durante un periodo de diez minutos, se debe bloquear la pantalla y suspender la sesión del usuario. El usuario si desea volver a entrar, debe autenticarse nuevamente.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.4 Control de Acceso al sistema.
Elemento:	4.4.1 Antivirus
El funcionario encargado deberá realizar consultas a los proveedores o casas de desarrollo de software con el fin de establecer las actualizaciones que puedan tener las diferentes aplicaciones, respaldando mediante una copia de seguridad las versiones anteriores del programa y evaluando su funcionamiento posterior a la instalación de la actualización.	
El funcionario encargado de soporte técnico, deberá visitar periódicamente fuentes de información relacionadas con la aparición de nuevos virus informáticos.	
El administrador del sistema deberá realizar un seguimiento continuo de los puertos qué se encuentran habilitados en el sistema con el fin de verificar que no se estén utilizando por algún tipo de virus.	
El Centro de Informática debe contar con herramientas para la búsqueda y corrección de virus, troyanos y puertas traseras.	
Solo se realiza descarga de archivos de redes externas, de acuerdo con los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo archivo que se obtenga de redes o dependencias externas al Centro de Informática.	
El Centro de Informática debe realizar revisiones periódicas de la información que almacena en sus computadoras, para evitar que archivos se encuentren infectados.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.4 Control de Acceso al sistema.
Elemento:	4.4.1 Antivirus
Los computadores del Centro de Informática y las dependencias relacionadas, deben tener instalado un antivirus que mantenga el sistema constantemente protegido, de manera que alerte automáticamente cuando se infecte.	
Los antivirus se deben actualizar por lo menos una vez a la semana, para evitar la infección por virus nuevos.	
Todo medio antes de ser leído debe ser vacunado.	
No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Universidad a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.	
El personal de las dependencias que tienen relación directa con servidores, deben estar capacitados frente a procedimientos, de identificación y eliminación de virus en correos electrónicos, medios magnéticos, páginas Web.	
Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al encargado de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.	
Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o Shareware, a menos que haya sido previamente aprobado por el Centro de Informática.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.5 Requerimientos Legales
Elemento:	4.5.1 Licencias
El personal encargado de la adquisición de software en la institución, debe tener conocimiento de la normatividad legal, frente a derechos de autor y licencias de software.	
Se debe realizar un inventario periódico del software instalado en los computadores de la institución, en el cual se especifique tipo de software, tipo de licencia, estado de la legalidad del software.	
Se debe especificar un inventario de licencias de software especificando: fecha de adquisición, documento que relacione su adquisición, tipo de licencia y caducidad de la licencia.	
La licencia debe especificar: • Número de equipos para los cuales se puede hacer uso de esta licencia. • Términos y alcances del COPYRIGHT. • País que protege mediante sus leyes la propiedad del software • La entrega de medios. • Propiedad intelectual del software	
Se debe establecer los términos para las actualizaciones del software así como la ejecución y cubrimiento de la garantía.	
Se prohíbe a los usuarios utilizar el software de la Universidad, para fines personales.	
Los usuarios deben comprometerse a no instalar en los equipos a su cargo, software que no este autorizado por la Universidad.	

4. SEGURIDAD LÓGICA	
Aspecto:	4.5 Requerimientos Legales
Elemento:	4.5.1 Licencias
Para uso de aplicativos se debe determinar la propiedad intelectual de los programas que utiliza y los términos de utilización del software.	
En el Centro de Informática, se debe evitar la instalación de software del cual no se tenga establecido su procedencia, proveedor, desarrollador o grupo de soporte técnico especializado, para evitar así software que provoque daños en los sistemas.	
Las licencias adquiridas por la Universidad deben estar respaldadas por un documento que especifique, tipo de licencia, fecha de inicio de la licencia, fecha de caducidad de la licencia, nombre del contacto de soporte técnico, teléfonos de contacto.	
Las licencias deben almacenarse en un lugar seguro, organizadas para facilitar su accesibilidad en caso que se requieran.	

5. SEGURIDAD EN EL PERSONAL	
Aspecto:	5.1 Funciones y Responsabilidades
Elemento:	5.1 Funciones y Responsabilidades
En el Centro de Informática debe existir una copia del manual de funciones y responsabilidades, establecidas para cada uno de los cargos asignados a esta dependencia.	
Los funcionarios del Centro de Informática deben tener pleno conocimiento de las funciones y responsabilidades que según el manual le correspondan.	
En el Centro de Informática se debe mantener una copia del documento de normas y políticas establecidas para esta dependencia.	
Es responsabilidad del Director del Centro de Informática de poner en conocimiento a los funcionarios de esta dependencia, la documentación correspondiente a manuales, normas y políticas.	
Los funcionarios del Centro de Informática deben cumplir a cabalidad con las normas y políticas instituidas en la dependencia.	
Los funcionarios del Centro de Informática serán responsables de todas las actividades que le correspondan, de igual manera de la información y equipos que tengan a su cargo.	
La institución debe informar por escrito de cualquier cambio en el manual de funciones y actualizar el documento.	

5. SEGURIDAD EN EL PERSONAL	
Aspecto:	5.2 Capacitación del Personal
Elemento:	5.2 Capacitación del Personal
Los funcionarios del Centro de Informática deben recibir capacitaciones en lo referente a seguridad informática y ser concientes de la importancia de la seguridad para garantizar la integridad, confiabilidad y confidencialidad de la información con la cual trabajan.	
En las carteleras del Centro de Informática, se fijaran avisos de seguridad llamativos, extraídos de revistas, periódicos, Internet, etc., que ilustren la importancia y la necesidad de mantener seguridad.	
Se debe establecer una línea de comunicación sobre seguridad, en la cual el personal pueda obtener sugerencias de seguridad y también pueda informar sobre violaciones de seguridad o actividades sospechosas.	
La Universidad de Nariño debe establecer programas de capacitación para todos los funcionarios de la Universidad, en el funcionamiento y manejo de equipos de seguridad provistos para incendios o inundaciones.	
La Universidad de Nariño establecerá planes de evacuación para todas las dependencias de la Universidad, en caso que sucediera algún desastre.	

5. SEGURIDAD EN EL PERSONAL	
Aspecto:	5.3 Ergonomía
Elemento:	5.3 Ergonomía
Los sitios de trabajo de los funcionarios deben tener una adecuada distribución de los equipos, dispositivos y herramientas que utilicen, además, deben dotarse con sillas ergonómicas, de manera que el usuario se coloque en la posición mas natural posible.	
Debe realizarse una distribución de trabajo equitativa entre los funcionarios del Centro de Informática, para evitar efectos de estrés o salud mental, ocasionados por la carga operativa.	
Los monitores de los computadores deben estar provistos de protectores de pantalla, en la medida de lo posible lograr que los funcionarios utilicen anteojos con protección para el monitor.	
El sitio de trabajo de los funcionarios deben contar con buena iluminación.	
El Centro de Informática debe contar con un mecanismo de ventilación.	
Los funcionarios del Centro de Informática, no deben estar expuestos a equipos ruidosos que excedan los 55 decibeles.	

12. CONCLUSIONES

- Para concluir este trabajo sería interesante que se piense un momento, en qué pasaría si el Rector no pudiera obtener un reporte consolidado de la información de la Universidad, o que a los estudiantes no se les pudiera entregar un certificado de estudios, que no estuviera disponible el servidor de correo electrónico o que los pagos a los trabajadores se retrasaran, que en el momento de comprar insumos no se supiera cual es la cantidad que se tiene en el inventario actual, estos se podrían ver como problemas simples para algunos, un poco críticos para otros, pero para la persona que esta involucrada en el proceso, que estos problemas sucedan, implicaría traumas en el desempeño de sus actividades, una mala inversión, perder un convenio o un trabajo en fin, se desencadenarían un sin número de problemas, ¿por qué?... sencillamente por que el mundo de hoy es el mundo de la información y los procesos sistematizados y computarizados, es por esto que la mejor conclusión que se puede obtener de este trabajo, es que se debe mantener la información disponible, confiable, e integra y que la manera de hacerlo es a través de la concientización, capacitación y a través de lineamientos claros de seguridad informática.

- El Centro de Informática de la Universidad de Nariño, es una dependencia regulada por la Vicerectoría Administrativa y asesorada por el Comité de Sistemas, encargada de adelantar soluciones de tipo tecnológico para las dependencias de la Universidad y que debe garantizar que los procesamientos de la información que administran se trabajen de forma segura y confiable.

- Los mecanismos de seguridad con los que cuenta el Centro de Informática no son los apropiados para reducir de manera significativa los riesgos asociados a la seguridad informática, ya que presenta inconvenientes en las áreas físicas (de instalaciones y construcción), desarrollo de software, redes de datos y redes eléctricas lo cual en un momento dado puede comprometer tanto la disponibilidad, como la integridad de la información que manejan las dependencias de OCARA, Recurso Humanos, Tesorería, Almacén y Contabilidad y puede llevar a que sea vulnerada la confidencialidad, estos tres aspectos son de sumo cuidado ya que para una institución educativa la información académica de los estudiantes, como la de los trabajadores y la relaciones de activos, pasivos procesos administrativos y demás son la base fundamental de funcionamiento.

- Las políticas de seguridad, son una herramienta transversal dentro de la Universidad ya que cubren todas las dependencias y funcionarios de la misma, es tan importante que un vigilante cumpla con los requisitos de seguridad al aplicar su conocimiento en su actividad diaria, como el trabajo de los desarrolladores al codificar las líneas de las aplicaciones, como también es vital que los usuarios que deben realizar el ingreso y administración de la información cumplan con los

requerimientos para mantener segura la información y el personal de mantenimiento realizando su labor oportunamente reduzca los riesgos de problemas en el hardware, el personal de redes eléctricas que manteniendo un optimo funcionamiento de las mismas evitando cortes o caídas, que interrumpan las labores de procesamiento y el personal que administra las redes de datos monitoreando y proyectando de manera adecuada el crecimiento y disponibilidad de la comunicación, es por estas muestras de actividades que la seguridad es uno de los ejes que debe mover el procesamiento de la información.

- Es importante que la Universidad cuente con un grupo interdisciplinario de personas con conocimientos en seguridad informática aplicados a las áreas como física (construcción e instalaciones), redes de datos, redes eléctricas, ingeniería de software, programación, Auditoría , quienes de forma constante realicen procesos de seguimiento a las diferentes actividades que involucran el procesamiento de la información, además este grupo debe tener la autonomía suficiente par poder realizar diagnósticos, Auditoría s o seguimiento en el momento que lo estipulen necesario.

- Las políticas de seguridad son lineamientos administrativos que respaldan los procesos operativos, es por esta razón que los directivos deben ser conscientes de su importancia y deben estar comprometidos con su implementación, brindando las herramientas y recursos necesarios para que esta tarea se consolide dentro de la Universidad.

- Es de vital importancia la implementación de políticas que establezcan los lineamientos, obligaciones y deberes de los funcionarios frente a la seguridad informática y concientizar de la importancia de su aplicación.

- La seguridad es un proceso de constante retroalimentación, dados los avances tecnológicos y la implementación de nuevas tecnologías y servicios y es un proceso de sinergia entre la parte operativa como lo son el Centro de Informática, el Aula de Informática, los mismos funcionarios y los administrativos que debe respaldar los procesos implementados y de mejoramiento de la seguridad.

- La creación del documento de políticas de seguridad, que se convierte en la base inicial para la implementación de lineamientos concretos sobre seguridad informática en la Universidad.

BIBLIOGRAFÍA

ALDEGANI, Gustavo miguel. Seguridad Informática MP EDICIONES Argentina, 1997.

BORGHELLO, Cristian. Tesis "Seguridad Informática: Sus Implicancias e Implementación". Argentina 2001.

ECHENIQUE G, José Antonio. Auditoría en Informática. McGrawHill, 2001.

HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 2.1.

MAIWALD Eric. Fundamentos de seguridad de redes. McGrawHill.

MARIO G. Piattini – Del Peso Emilio., Auditoría Informática Un Enfoque Practico. Alfaomega, 1998.

MCCLURE Stuart- SCAMBRAY Joel – KURTZ George. HACKERS Secretos y Soluciones para la seguridad de redes. McGrawHill.

Microsoft, Fundamentos de Redes Plus, Curso Oficial de Certificación MCSE. McGrawHill.

PINILLA F, Dagoberto. Auditoría Informática un Enfoque Operacional. Ecoe ediciones.

PORTILLA CH., Gloria - GOMEZ L., Delio. Evaluación al Proceso Sistematizado de Registro y Control Académico de la Universidad de Nariño. Universidad Antonio Nariño – Universidad Mariana. San Juan de Pasto, 1995.

PRESSMMAN Roger, S.: *Ingeniería del Software. Un Enfoque Práctico.* McGraw-Hill,,

TANENBAUM Andrew S.: Redes de Computadoras. Prentice Hall.

VILLA LOBOGUERRRERO, Horacio. Guía de Fundamentos de Auditoría de Sistemas. Universidad Antonio Nariño.

ANEXO A
ARCHIVO CORRIENTE

SEGURIDAD LÓGICA

Cuestionario de Evaluación a la seguridad en la aprobación, planeación y gestión del proyecto.	SLC01/SLC02
HALLAZGO 01 “No existe una adecuada planeación…”	SLH01
Cuestionario de evaluación a la etapa de análisis.	SLC03
Cuestionario de evaluación a la etapa de diseño.	SLC04
HALLAZGO 02 “No existe personal de auditoria …”	SLH02
HALLAZGO 03 “La encriptación de contraseñas... ”	SLH03
Cuestionario de evaluación a la seguridad en la etapa de desarrollo.	SLC04
HALLAZGO 04 “no se tiene establecidos estándares...”	SLH04
HALLAZGO 05 “Las aplicaciones no tienen establecido...”	SLH05
HALLAZGO 06 “El sistema no advierte al usuario...”	SLH06
HALLAZGO 07 “Los usuarios no tienen opción para...”	SLH07
HALLAZGO 08 “El código fuente de las aplicaciones no es revisado”	SLH08
Cuestionario de evaluación a la seguridad en la etapa de implementación.	SLC05
HALLAZGO 09 “No existe personal de auditoria de sistemas que acompañe...”	SLH09
HALLAZGO 10 “Las pruebas realizadas en las aplicaciones no se encuentran documentadas...”	SLH10
HALLAZGO 11 “No existe un documento que establezca...”	SLH11
HALLAZGO 12 “Los funcionarios de las dependencias, no cuentan...”	SLH12
Cuestionario de evaluación a la seguridad en copias de seguridad.	SLC06
HALLAZGO 13 “Las copias de seguridad no se almacenan...”	SLH13
HALLAZGO 14 “No existe un documento que especifique los pasos...”	SLH14
HALLAZGO 15 “Las copias de seguridad no se guardan en forma...”	SLH15
Cuestionario de evaluación de la adquisición de software para la Universidad de Nariño.	SLC07
Cuestionario de los requerimientos legales en la utilización del software en el Centro de Informática.	SLC08
HALLAZGO 16 “El aula de informática realizo una revisión del software...”	SLH16

Cuestionario de evaluación de manejo de antivirus en el centro de informática.	SLC09
HALLAZGO 17 “El tiempo para la realización de la actualización...”	SLH17
HALLAZGO 18 “No se tiene restricción sobre los archivos...”	SLH18
Cuestionario de evaluación a la seguridad del sistema operativo.	SLC10
HALLAZGO 19 “El sistema operativo que maneja actualmente...”	SLH19
Cuestionario de evaluación del manejo de bases de datos en el centro de informática.	SLC11
HALLAZGO 20 “La información que se aloja en las bases de datos...”	SLH20
HALLAZGO 21 “A pesar de que los procesos para la realización de las copias de seguridad...”	SLH21
HALLAZGO 22 “a pesar de que los procesos para la restauración...”	SLH22
Cuestionario de evaluación servicios de Internet.	SLC12/ SLC13
HALLAZGO 23 “El proveedor de Internet no presta servicios...”	SLH23
HALLAZGO 24 “No existen lineamientos definidos...”	SLH24
HALLAZGO 25 “No se realiza un seguimiento...”	SLH25
Evidencias	SLEV01-SLEV25

SEGURIDAD DE PERSONAL

Cuestionario de capacitación de personal	SPC01
HALLAZGO 01 “Muchos usuarios de las dependencias, no han recibido...”	SPH01
HALLAZGO 02 “No se entrega manual de usuario...”	SPH02
HALLAZGO 03 “Los funcionarios no tienen conocimiento del manual de funciones...”	SPH03
HALLAZGO 04 “No existe manual de procedimientos...”	*SPH04*
Cuestionario de evaluación de la ergonometria y bienestar laboral Centro de Informática.	SPC02
HALLAZGO 05 “los computadores del Centro de Informática no esta provistos de protectores de pantalla...”	SPH05
HALLAZGO 06 “Los trabajadores del centro de informática tienen carga...”	SPH06
Cuestionario de evaluación del control de acceso a las instalaciones del centro de informática.	SPC03/ SPC04

HALLAZGO 07 “El centro de informática no dispone de un sistema...”	SPH07
HALLAZGO 08 “El personal de la oficina del Centro de Informática...”	SPH08
HALLAZGO 09 “No se tiene establecido un control...”	SPH09
HALLAZGO 10 “El personal ajeno a la institución...”	SPH10
HALLAZGO 11 “El Centro de Informática, no dispone...”	SPH11
HALLAZGO 12 “El edificio donde se localiza el Centro de Informática...”	SPH12
HALLAZGO 13 “El personal de vigilancia, no esta capacitado...”	SPH13
Evidencias	SPEV01-SPEV12

SEGURIDAD FÍSICA

Cuestionario de evaluación de la ubicación y construcción del Centro de Informática.	SFC01-SFC05
HALLAZGO 01 “El Centro de Informática de la Universidad de Nariño, se ubica en el primer...”	SFH01
HALLAZGO 02 “El Centro de Informática de la Universidad de Nariño, se encuentra distante...”	SFH02
HALLAZGO 03 “El diseño y distribución de espacios del Centro de Informática...”	SFH03
HALLAZGO 04 “En el Centro de Informática y en la oficina...”	SFH04
HALLAZGO 05 “No existen los planos de la red de datos...”	SFH05
HALLAZGO 06 “No existen los planos de la red eléctrica...”	SFH06
HALLAZGO 07 “Las divisiones internas del Centro de Informa, al igual que muebles...”	SFH07
HALLAZGO 08 “Las divisiones internas del Centro de Informa son de material...”	*SFH08*
HALLAZGO 09 “La ventana y la puerta de acceso principal...”	SFH09
HALLAZGO 10 “El Centro de Informática no esta dotado...”	SFH10
HALLAZGO 11 “El Centro de Informática cuenta con dos chapas...”	SFH11
HALLAZGO12 “ Se encuentran fisuras en la masilla que asegura...”	*SFH12*
HALLAZGO13 “Es notable que la distribución de espacios...”	*SFH13*
HALLAZGO14 “El Centro de Informática no dispone de suficiente espacio...”	*SFH14*
HALLAZGO15 “El Centro de Informática no dispone de un espacio asignado...”	*SFH15*
HALLAZGO16 “El Centro de Informática no dispone de un área...”	*SFH16*

Cuestionario de evaluación del control ambiental en el Centro de Informática.	SFC06
HALLAZGO 17 “El Centro de Informática no dispone de un termómetro...”	SFH17
HALLAZGO 18 “El cuarto de maquinas y el área de trabajo de los programadores...”	SFH18
HALLAZGO 19 “El Centro de Informática no dispone de un sensor para controlar...”	SFH19
Cuestionario de evaluación de la seguridad frente a desastres en el Centro de Informática.	SFC07-SFC09
HALLAZGO 20 “El Centro de Informática y el perímetro...”	SFH20
HALLAZGO 21 “El Centro de Informática dentro de su dotación...”	SFH21
HALLAZGO 22 “En el primer piso del edificio, donde se ubica...”	SFH22
HALLAZGO 23 “En el edificio donde se localiza el Centro de Informática...”	SFH23
HALLAZGO 24 “El personal del Centro de Informática no se encuentra capacitado...”	SFH24
HALLAZGO 25 “El cuerpo de bomberos no ha sido informado...”	SFH25
HALLAZGO 26 “La salida del Centro de Informática y el Bloque Administrativo no se encuentra...”	SFH26
HALLAZGO 27 “Las divisiones internas del Centro de Informática...”	SFH27
HALLAZGO 28 “No se dispone de una bomba para extracción...”	SFH28
HALLAZGO 29 “Los hidrates son una medida de aseguramiento...”	SFH29
HALLAZGO 30 “En caso de inundación se corre el riesgo...”	SFH30
HALLAZGO 31 “El Centro de Informática no tiene a la vista,...”	SFH31
Cuestionario de evaluación de la seguridad en equipos en el Centro de Informática.	SFC10/ SFC11
HALLAZGO 32 “Los servidores con que cuenta el Centro de Informática, no son...”	SFH32
HALLAZGO 33 “El Centro de Informática no cuenta con planta eléctrica...”	SFH33
HALLAZGO 34 “los equipos del Centro de Informática no reciben mantenimiento...”	SFH34
HALLAZGO 35 “Los equipos del Centro de Informática se encuentran destapados...”	SFH35
HALLAZGO 36 “En el bloque administrativo, no existe control...”	SFH36
HALLAZGO 37 “La limpieza al Centro de Informática se realiza...”	SFH37
HALLAZGO 38 “No existe una política que prohíba el consumo...”	SFH38
Evidencias	SFEV01-SFEV34

Cuestionario de evaluación del control de acceso dependencias	SFDEC01-SFDEC04
HALLAZGO 01 “El personal de las oficinas de ...”	SFDEH01
HALLAZGO 02 “El personal ajeno a la institución, que ingresa...”	SFDEH02
HALLAZGO 03 “Las oficinas de Ocara, tesoreria ...”	SFDEH03
HALLAZGO 04 “La puerta de acceso principal...”	SFDEH04
HALLAZGO 05 “Las ventanas internas de las oficinas...”	SFDEH05
HALLAZGO 06 “El edificio donde se localiza el bloque administrativo...”	SFDEH06
Cuestionario de evaluación del control de acceso dependencias	SFDEC05-SFDEC07
HALLAZGO 07 “Las instalaciones de Ocara, ...”	SFDEH07
HALLAZGO 08 “El gabinete contra incendios mas cercano...”	SFDEH08
HALLAZGO 09 “El personal de las oficinas de Ocara, ...”	SFDEH09
HALLAZGO 10 “El personal de las oficinas de Ocara, Almacén, Recursos Humanos, Contabilidad, no se encuentra capacitado ...”	SFDEH10
Cuestionario de evaluación del control de acceso dependencias	SFDEC08-SFDEC10
HALLAZGO 11 “Los equipos de las dependencias no reciben...”	SFDEH11
HALLAZGO 12 “No existe control de la entrada y salida...”	SFDEH12
HALLAZGO 13 “No existe una política que prohíba el consumo...”	SFDEH13
Evidencias	SFDEV01-SFDEV011

SEGURIDAD ELÉCTRICA

Cuestionario de evaluación de la red eléctrica del Centro de Informática	SEC01/ SEC02
HALLAZGO 01 “El Centro de Informática no cuenta con un pararrayo...”	SEH01
HALLAZGO 02 “No se realizan revisiones, ni mantenimientos periódicos...”	SEH02
HALLAZGO 03 “Algunos equipos instalados en las oficinas...”	SEH03
HALLAZGO 04 “Se aprecia que existen reguladores eléctricos...”	SEH04
HALLAZGO 05 “Se presenta problemas en las conexiones...”	SEH05
HALLAZGO 06 “Las redes eléctricas no se encuentran señalizadas...”	SEH06
HALLAZGO 07 “Se presentan sectores en donde se evidencia...”	SEH07
Cuestionario de evaluación del mantenimiento de la red eléctrica.	SEC03
HALLAZGO 08 “Las conexiones eléctricas no reciben...”	*SEH08*
HALLAZGO 09 “Las reparaciones realizadas a los daños...”	SEH09

HALLAZGO 10 “Las conexiones de puesta a tierra...”	SEH10
Cuestionario de evaluación del mantenimiento de la red eléctrica.	SEC04/ SEC05
HALLAZGO12 “El Centro de Informática no cuenta con un sistema...”	*SEH11*
Evidencias	SEEV01-SEEV11

SEGURIDAD EN REDES

Cuestionario de evaluación a la administración de red y cableado	SRC01/ SRC02
HALLAZGO 01 “El Centro de Informática no cuenta con un diseño...”	SRH01
HALLAZGO 02 “No existe un documento en el que se especifique...”	SRH02
HALLAZGO 03 “Existen dispositivos que no se encuentran...”	SRH03
HALLAZGO 04 “Existen tramos de cableado...”	SRH04
HALLAZGO 05 “Existen equipos que se encuentran conectados...”	SRH05
HALLAZGO 06 “Se encuentran sectores de cableado que no...”	SRH06
HALLAZGO 07 “Se encuentran puntos críticos en...”	SRH07
HALLAZGO 08 “Los puntos de red presentan problemas...”	SRH08
Cuestionario de evaluación a la administración de red y cableado	SRC03/ SRC04
HALLAZGO 09 “No se realiza mantenimiento preventivo...”	SRH09
HALLAZGO 10 “Los problemas ocurridos en el mantenimiento...”	SRH10
HALLAZGO 11 “Se utilizan equipos que han presentado daños...”	SRH11
Evidencias	SREV01-SREV11

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN A LA SEGURIDAD EN EL DESARROLLO DEL SOFTWARE

OBJETIVOS

-Verificar que el desarrollo de software se haga cumpliendo con todas las etapas de una metodología determinada ó de acuerdo a lineamientos establecidos por la institución.

-Evaluar que el proyecto cuente con una planeación adecuada que lo haga realizable.
-Comprobar que las necesidades y sugerencias de usuarios y agentes de auditoria sean tomadas en cuenta.
-Controlar que el acceso a la información se realice únicamente por el personal autorizado
-.Evaluar que la aplicación sea auditable de manera que incluya controles y pistas de auditoría.

EVALUACIÓN A LA SEGURIDAD EN LA APROBACIÓN, PLANEACIÓN Y GESTIÓN DEL PROYECTO	**REF:** SLC01 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**

Los sistemas se desarrollan por solicitud escrita de parte del comité de sistemas?	X			
Existe una orden de aprobación del proyecto generada por un órgano competente?	X			
Son definidos plenamente los requerimientos de información en la fase preliminar del proyecto?	X			
Existe un documento que manifieste la aprobación del proyecto?	X			
En el documento de aprobación están definidos de forma clara y precisa los objetivos?	X			
En el documento de aprobación están definidos de forma exacta las restricciones de tiempo y recursos?		X		SLH01

EVALUACIÓN A LA SEGURIDAD **EN LA APROBACIÓN, PLANEACIÓN Y** **GESTIÓN DEL PROYECTO**	**REF:** SLC02 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se establecen términos para la entrega del proyecto como: Periodos de revisión? Fecha de entrega? Reuniones de presentación?	 X X X			
Existe un cronograma de actividades que estime el tiempo requerido para el desarrollo de la aplicación?	X			
El proyecto cuenta con una planeación que lo haga realizable?	X			
En la planeación se define el modelo de desarrollo de software a utilizar en función de sus características y restricciones?	X			
El personal técnico asignado al desarrollo es competente?	X			

Si participa personal externo, el perfil profesional es adecuado a las exigencias del proyecto?	X			
La documentación que se recolecta del proyecto es completa?	X			
La información está catalogada perfectamente para accesos posteriores?	X			

EVALUACIÓN A LA APROBACIÓN, PLANEACIÓN Y GESTIÓN DEL PROYECTO DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH01 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 01

No existe una adecuada planeación de los proyectos, ya que no se define con exactitud las restricciones de tiempo y recursos que hacen necesarios para el completo cumplimiento del proyecto. Es evidente que la documentación de los programas no se logra realizar por el escaso tiempo que tienen los programadores para dar entrega del mismo.
Las aprobaciones no se realizan de forma escrita.

Evidencia: SLEV01a – SLEV01b

RECOMENDACIÓN

La planeación del proyecto debe tener en cuenta el tiempo y recursos necesarios para el proceso de desarrollo y la realización de la documentación correspondiente.

Los documentos de aprobación deben ser elementos indicadores de los avances del proyecto, estos documentos deben contener los objetivos, las fechas de entrega y los recursos que serán necesarios para el desarrollo del proyecto.

El Comité de Sistemas debe realizar un estudio de las necesidades del Centro

de Informática frente a personal que se dedique a funciones especificas como de análisis, diseño, mantenimiento, seguridad, entre otros.

FORMATO DE CONTROL INTERNO **EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO**				
EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE ANÁLISIS**	**REF:** SLC03 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se ha planteado una metodología específica para el análisis de sistemas?	X			
Se cumplen los lineamientos establecidos en la metodología?	X			
El proceso de análisis obedece a estándares establecidos para el análisis de sistemas?	X			
Se realiza un adecuado levantamiento de información para el entendimiento de los requerimientos del sistema?	X			
Se realizan entrevistas a usuarios	X			
El analista atiende las necesidades del usuario?	X			
Se encuentra debidamente documentado todo el proceso de análisis?	X			

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**REF:** SLC04 **Elaboró:** M.C.T y E.A.F **Fecha:** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Participa personal de auditoria para establecer controles dentro de la aplicación?		X		SLH02
Se contempla en el diseño un modulo de seguridad?	X			
El módulo de seguridad establece control de acceso de usuarios, a través de un nombre de usuario y contraseña?	X			
Existe un modelo de encriptación de claves?		X		SLH03
Se establecen privilegios de usuario para acceso al sistema?	X			
Existe un registro de entradas al sistema que especifique:				
Usuario?	X			
Fecha de ingreso?	X			
Hora de ingreso?	X			
Archivos accesados?	X			
Acción realizada?	X			
Valor anterior del registro?	X			
Nuevo valor del registro?	X			
Existe documentación del diseño del modulo de seguridad.		X		SLH01
Se garantiza que los datos eliminados por los usuarios, se guarden en otro archivo durante un tiempo determinado?	X			
Se realizan actas donde se plasme los compromisos y cambios acordados con el auditor?			X	

Se realiza seguimiento a la seguridad implementada en el sistema?	X			

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH02 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 02	
No existe personal de auditoria de sistemas en la dependencia de Control Interno, que participe de los procesos de sistematización que adelanta el Centro de Informática, las revisiones de auditoria se enfoca a la revisión de los reportes que generan los sistemas, en lo relacionado a la parte financiera. Evidencia: SLEV02	
RECOMENDACIÓN	
Incluir dentro del personal de Control Interno un especialista en auditoria informática, que realice los controles de seguridad correspondientes a la sistematización de los procesos de la Universidad.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH03 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 03	
La encriptación de contraseñas, se realiza a través del Sistema Operativo en el acceso de los usuarios, sin embargo las claves de acceso a las aplicaciones no se encriptan por ningún mecanismo. Evidencia: SLEV03	
RECOMENDACIÓN	
Utilizar un mecanismo de encriptación aprobado por la dirección del Centro de Informática, para proteger las claves de acceso a las aplicaciones de los usuarios de los sistemas.	

FORMATO DE CONTROL INTERNO **EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO**				
EVALUACIÓN A LA SEGURIAD **EN LA ETAPA DE DESARROLLO**	**REF:** SLC05 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se encuentra el programa documentado internamente de manera que describa de forma general el funcionamiento de: El programa? Rutinas? Variables?	 X X X			
Los programas poseen internamente sus propios procedimientos que permitan recuperar información en caso que ocurran fallos en el sistema?	X			
Existen controles adecuados para identificar y corregir ingreso de datos?	X			
Se mantienen copias de los fuentes programas durante el desarrollo de las aplicaciones?	X			
Se encuentran definidos estándares para la programación?		X		SLH04
El módulo de seguridad especificado en el diseño es coincidente con el desarrollo del programa?	X			
Los usuarios entran al sistema a través de un nombre de usuario y contraseña?	X			
Se evita la visibilidad de la contraseña?	X			
Se realiza control de contraseña de los usuarios mediante el programa?		X		SLH05
El programa emite mensajes que sugieran cambio de contraseña a los usuarios?		X		SLH06

Existe dentro del menú de usuario la opción que permita cambio de contraseña?		X		SLH07
Existe un registro de fecha y hora del cambio de contraseñas?	X			
Se realiza revisión del código fuente por parte de personal especializado en programación?		X		SLH08

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH04 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 04	
No se tienen establecidos estándares propios para el desarrollo de aplicaciones que especifiquen los lineamientos que los desarrolladores deben seguir para que la programación se encuentre unificada. Evidencia: SLEV04	
RECOMENDACIÓN	
Establecer lineamientos de desarrollo en los que se especifique indicadores que permitan realizar seguimiento al desarrollo de las aplicaciones y que ayuden a nuevos programadores a comprender la programación que se esta realizando; como son los casos de nombramiento estándar de variables, nombramientos para rutinas y funciones entre otras.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH05 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 05	
Las aplicaciones no tienen establecido control de las contraseñas de los usuarios por lo que no se realiza cambio periódico de contraseñas, ni tampoco validación de las mismas. Evidencia: SLEV05a – SLEV05b	
RECOMENDACIÓN	
Concientizar a los usuarios de la importancia de realizar cambio de contraseña periódicamente o realizarlo inmediatamente sospeche que otra persona logró visualizar su clave. Establecer que las aplicaciones realicen control de cambio de contraseña y además que las contraseñas se validen frente a número de caracteres, palabras reservadas y que sean estrictamente de combinación alfanumérica para mayor seguridad. El cambio de contraseña debe realizarse por lo menos una vez al mes.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH06 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 06	
El sistema no advierte al usuario de la necesidad de realizar cambio de contraseña. Evidencia: SLEV06	
RECOMENDACIÓN	
Incluir dentro de las Aplicaciones, mensajes a los usuarios advirtiendo del cambio de contraseña.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH07 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 07	
Los usuarios no tienen la opción para realizar cambio de contraseña directamente desde su menú de trabajo, esta tarea la realiza el administrador del sistema a petición del usuario. Evidencia: SLEV07	
RECOMENDACIÓN	
Incluir dentro del menú de los usuarios la opción para realizar cambio de contraseña, esta medida agiliza el proceso de cambio de contraseña.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH08 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 08	
El código fuente de las aplicaciones desarrolladas no es revisado por personas especializadas que verifiquen la integridad del código. Evidencia: SLEV08	
RECOMENDACIÓN	
Asignar una persona que revise la codificación de las aplicaciones en especial cuando son desarrolladas por programadores externos de la Universidad como las aplicaciones desarrolladas por estudiantes como trabajo de grado, a fin de evitar en el código líneas maliciosas que puedan alterar los sistemas.	

FORMATO DE CONTROL INTERNO **EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO**				
EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE IMPLEMENTACIÓN**	**REF:** SLC06 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Pruebas				
Se realizan pruebas preliminares al programa una vez se encuentra terminado?	X			
El personal de auditoria realiza pruebas de verificación a las aplicaciones?		X		SLH09
Se documentan los resultado de las pruebas?		X		SLH10
Para probar los programas se utilizan datos de prueba?	X			
Existe un documento de aprobación que especifique, el correcto funcionamiento del programa?		X		SLH11
Entrenamiento a Usuarios				
Los usuarios han recibido la formación necesaria para el manejo de la aplicación?	X			
Tienen los usuarios en su poder la documentación suficiente para la operación del programa?		X		SLH12
Servicio post-implementación.				
Se atiende oportunamente los problemas que los usuarios tienen frente al sistema?	X			
Se realiza mantenimiento a la aplicación?	X			
Se realizan copias de seguridad de forma periódica?	X			

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH09 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 09	
No existe personal de auditoría de sistemas que realice acompañamiento a las pruebas del programa, de manera que verifique el correcto funcionamiento de los controles de seguridad implementados en el programa. Evidencia: SLEV09	
RECOMENDACIÓN	
Incluir en los procedimientos de prueba a personal especializado en auditoria de sistemas que verifique la implementación y correcto funcionamiento de los controles de seguridad incluidos en el programa.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH10 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 10	
Las pruebas realizadas a las aplicaciones no se encuentran documentadas en donde se constate la realización de las pruebas y los resultados de las mismas. Evidencia: SLEV10	
RECOMENDACIÓN	
Realizar un documento en el que se establezcan las fechas en que se realizan las pruebas, personal que participo, descripción de las pruebas realizadas, resultados obtenidos.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH11 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 11	
No existe un documento en el que se establezca el correcto funcionamiento del sistema y se apruebe su instalación. Evidencia: SLEV11	
RECOMENDACIÓN	
Generar un documento que establezca que el software se encuentra listo para su implementación.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH12 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 12	
Los funcionarios de las dependencias, no cuentan con manuales de usuario que los oriente en la operatividad del sistema. Evidencia: SLEV12	
RECOMENDACIÓN	
Se recomienda entregar manuales de usuarios claros y específicos, de todas las aplicaciones que manejen los usuarios y entregar copia a ellos a las dependencias que corresponda.	

FORMATO DE CONTROL INTERNO **EVALUACIÓN DE LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO**				
EVALUACIÓN DE LA SEGURIDAD **EN COPIAS DE SEGURIDAD**	**REF:** SLC07 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se realizan copias de seguridad de la información que administra el Centro de Informática?	X			
Existen responsables de la realización de las copias de seguridad?	X			
Se realizan copias de seguridad periódicamente?	X			
Existe copia de seguridad dentro de la oficina del Centro de Informática?	X			
Existe una copia de seguridad fuera de las instalaciones de la Universidad?	X			
Las copias de seguridad se almacenan en áreas restringidas?		X		SLH13
El lugar donde se almacenan las copias de respaldo, garantizan la seguridad de los medios?		X		SLH13
Existen control para el acceso a las copias de respaldo?		X		SLH13
Esta definidos por escrito los procedimientos a seguir para la restauración de las copias?		X		SLH14
Se maneja encripción en las copias de seguridad?		X		SLH15

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH13 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 13	
Las copias de seguridad no se almacenan en áreas restringidas, generalmente se guardan en los escritorios de los funcionarios, facilitando su acceso. Evidencia: SLEV13	
RECOMENDACIÓN	
Establecer un área dispuesta para el almacenamiento de las copias de seguridad, al cual solo personal autorizado pueda acceder, ubicado en un sito restringido y aseguradas con mecanismos de seguridad y en el cual se pueda realizar una correcta organización.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH14 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 14	
No existe un documento que especifique los pasos y procedimientos a seguir en caso de que sea necesaria la restauración de una copia de seguridad. Evidencia: SLEV14	
RECOMENDACIÓN	
Documentar claramente los procesos de restauración de copias de seguridad, colocar en conocimiento del documento a la persona responsable del esta clase de procesos y además capacitar a una personal adicional en la realización de estos procedimientos.	

EVALUACIÓN A LA SEGURIDAD **EN LA ETAPA DE DISEÑO**	**R.P.T. :** SLH15 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 15	
Las copias de seguridad no se guardan de forma encriptada, únicamente se realiza la copia de seguridad y se almacena en el medio. Evidencia: SLEV15	
RECOMENDACIÓN	
Encriptar la copia de seguridad teniendo en cuenta los siguientes parámetros, encripción de los datos, encripción de estructuras y datos, encripción del archivo de la copia.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Verificar que la adquisición de software se realice teniendo en cuenta parámetros de seguridad que garanticen la protección de la información y la continuidad de las funciones de la institución.

EVALUACIÓN DE LA ADQUISICIÓN DE SOFTWARE PARA LA UNIVERSIDAD DE NARIÑO	**REF:** SLC08 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se realiza un estudio de las necesidades de la institución, para determinar la adquisición del software adecuado?	X			
Para la adquisición de software, se considera que contenga módulo de auditoria en el que registre todas las actividades realizadas por los usuarios?	X			
Se considera que el software para adquisición realice control de acceso a usuarios?	X			

Se estima que el software contemple opciones para realizar backups de la información?	X			
Para adquirir software se tienen en cuenta los recursos de hardware disponibles en la Universidad?	X			
Se tienen en cuenta los requerimientos legales?	X			

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Verificar la legalidad del software instalado en los equipos de trabajo del centro de informática.

EVALUACIÓN DE LOS REQUERIMIENTOS LEGALES EN LA UTILIZACIÓN DEL SOFTWARE EN CENTRO DE INFORMÁTICA	**REF:** SLC09 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004

A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Existe una relación de software instalado?	X			
La totalidad de software instalado en los equipos del centro de informática, se encuentra licenciado?		X		SLH16

Las licencias utilizadas para legalizar los programas en los equipos, son las adecuadas según el tipo de licencia?	X			
La disponibilidad de los medios se realiza bajo autorización del personal responsable de ellos?	X			
Existe control sobre los medios de los programas instalados?	X			

EVALUACIÓN A LA SEGURIDAD EN LA ETAPA DE DISEÑO	**R.P.T. :** SLH16 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 16	
El aula de informática realizó una revisión del software instalado en los computadores de la Universidad en el año 2003 según lo establecido por el comité de sistemas en el acta 006 de 5 marzo de 2003. Esta revisión se realizo en las dependencias, excepto en el Centro de Informática, en donde se encuentra software que no se encuentra legalizado, y que se ha hecho necesaria su instalación para realizar procesos propios de la dependencia. **En el Aula de Informática se encuentran almacenadas las fichas de esta medida de control a las dependencias, pero no se encontró la correspondiente a las dependencias del bloque administrativo, sin embargo los funcionarios de las dependencias y el coordinador del Aula certifican su realización.** Evidencia: SLEV16	

RECOMENDACIÓN
Controlar la instalación de software mediante revisiones periódicas a la totalidad de las dependencias, establecer las necesidades específicas de software del Centro de Informática para el normal desarrollo de sus funciones, implementar herramientas de software libre.

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Verificar que los sistemas no se encuentren expuestos a fallas ocasionadas por software antivirus.

EVALUACIÓN DE MANEJO DE ANTIVIRUS EN EL CENTRO DE INFORMÁTICA	**REF:** SLC10 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Existen normas para que los usuarios realicen una revisión con antivirus antes de leer disquetes o archivos que llegan?	X			
Existen instalado en los equipos software antivirus?	X			
La versión del antivirus se encuentra actualizada?	X			
Se revisa periódicamente las actualizaciones del antivirus suministradas por el proveedor?	X			
El tiempo para el desarrollo de las actualizaciones es el adecuado?		X		SLH17
Existe un programa para el control de gusanos, espías y troyanos?	X			
Se mantienen actualizados los sistemas con parches de seguridad?	X			
Se prohíbe las descargas de archivos por Internet?		X		SLH18

Se vacunan los medios externos antes de ser leídos?	X			
El software antivirus cuenta con licencia?	X			

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH17 **Fecha :** Marzo/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 17	
El tiempo para la realización de la actualización de los antivirus es demasiado alta, teniendo el cuenta que los equipos se encuentran conectados a Internet. **EVIDENCIA :** SLEV17	
RECOMENDACIÓN	
La recomendación es que el proceso de actualización de los antivirus o programas para protección contra gusanos, troyanos, se realice a diario o por lo menos una vez en el mes.	

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH18 **Fecha :** Noviembre/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 18	
No se tiene restricción sobre los archivos que se descargan de Internet. Evidencia : SLEV18	
RECOMENDACIÓN	
Se recomienda bloquear la descarga de programas y música, de ser necesario este servicio, se debe realizar una solicitud directa a una persona designada para tal fin, quien evaluara la información a descargar, descartando problemas de virus, gusanos, troyanos.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LÓGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN A LA SEGURIDAD DEL SISTEMA OPERATIVO

OBJETIVOS

-Controlar el acceso de personal autorizado al sistema y recursos del mismo.

-Verificar la instalación de herramientas de seguridad previstas por el fabricante del sistema.
-Comprobar que el Sistema Operativo existente brinda la mayor seguridad a la información.

EVALUACIÓN A LA SEGURIDAD **DEL SISTEMA OPERATIVO**	**REF:** SLC11 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004

A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se encuentran instaladas herramientas de seguridad propias del sistema?				
El Sistema Operativo requiere de ingreso de password?	X			
El password del Sistema Operativo utiliza algún método de encriptación?	X			
Se encuentran protegidas las librerías del sistema?				
El Sistema Operativo tiene la correspondiente licencia de uso?		X		SLH19
Para la adquisición de Sistema Operativo se tienen en cuenta parámetros de seguridad?	X			

El sistema operativo tiene mecanismos de recuperación para restablecer el sistema en caso que este se caiga?	X			
Se protege al sistema realizando las pruebas en un servidor de pruebas?	X			
Existe un control de permisos a usuarios sobre los archivos?	X			
Se encuentran cerrados los puertos no utilizados del sistema?	X			
Existe un control sobre los puertos habilitados?	X			

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH19 **Fecha :** Noviembre/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 19	
El Sistema Operativo que maneja actualmente el Centro de Informática Unix 5.05, no tiene la licencia correspondiente de uso, puesto que fue concedida a la Universidad de Nariño por Corponariño, mediante acuerdos que no se definieron específicamente entre las directivas. **Evidencia: SLEV19**	
RECOMENDACIÓN	
Realizar una planeación por parte del Comité de Sistemas, para legalizar el uso del actual Sistema Operativo.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD LOGICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Establecer las medidas de seguridad que se toman en cuenta para el diseño y trabajo con bases de datos.

EVALUACIÓNEN EL MANEJO DE BASES DE DATOS EN EL CENTRO DE INFORMÁTICA	**REF:** SLC12 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
El diseño de la base de datos contempla tablas de auditoria?	X			
Las tablas de auditoria registran los accesos de los usuarios al sistema?	X			
Las tablas de auditoria registran las actividades realizadas por los usuarios del sistema?	X			
El modelo de la base de datos contempla : Tablas para control de acceso? Como tablas de privilegios? Claves?	 X X X			
La información que se aloja en la base de datos se encuentra encriptada?		X		SLH20
Se realiza control de eliminación de datos?	X			
Se realiza control de modificación de datos?	X			

Se tiene licencia del motor de la base de datos?	X			
Se realizan procedimientos para la realización de copias de seguridad?	X			
Estos procedimientos de copias, se encuentran por escritos?		X		SLH21
Existen procedimientos para la recuperación de base de datos?		X		SLH22

EVALUACIÓN A LA SEGURIDAD EN BASES DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH20 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 20	
La información que se aloja en las bases de datos no se guarda de manera encriptada. EVIDENCIA: SLEV20	
RECOMENDACIÓN	
Dada la importancia y la delicadeza de la información se recomienda manejar procesos de encripción para el almacenamiento de la información en las bases de datos.	

EVALUACIÓN A LA SEGURIDAD EN BASES DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH21 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 21	
A pesar de que los procesos para la realización de las copias de seguridad se realizan y son de pleno conocimiento de los funcionarios, no existe documentación sobre los procedimientos necesarios para su realización. EVIDENCIA: SLEV21	
RECOMENDACIÓN	
Se recomienda documentar los procesos para la realización de copias de seguridad, estableciendo días para la copia, hora, responsables, medios en los que se realiza, archivos a los que se realiza la copia, ubicación de los medios. Además se debe relacionar los procedimientos para la restauración de las copias de seguridad.	

EVALUACIÓN A LA SEGURIDAD EN BASES DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH22 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 22	
A pesar de que los procesos para la restauración se ha realizado sobre de las copias de seguridad que se tienen, no existe documentación sobre los procedimientos necesarios para su realización. EVIDENCIA: SLEV22	
RECOMENDACIÓN	
Se recomienda documentar los procesos para la restauración de copias de seguridad, estableciendo que copia de seguridad hay que instalar, que prerrequisitos se necesitan y los demás proceso que sean necesarios para la restauración del sistema.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LOS SERVICIOS DE INTERNET DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Establecer las medidas de seguridad que se toman en cuenta para la seguridad en la prestación de servicios de Internet.

EVALUACIÓN SERVICIOS DE INTERNET	**REF:** SLC13 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
ASUNTO	**SI**	**NO**	**N.A**	**R.P.F**
Existe un responsable de la administración de los servicios de Internet?	X			
se cuenta con servidores dedicados para los servicios de Internet ?	X			
Se cuenta con equipos de respaldo para realizar restaurar servicios en el momento de problemas en los servidores principales ?	X			
El proveedor de Internet presta servicios para garantizar la información se transporte de manera segura ?		X		SLH23
Existen unos lineamientos definidos por escrito que determinen los procesos de desarrollo de aplicaciones Web ?		X		SLH24
Se realiza un seguimiento detallado de las soluciones web desarrolladas por personas ajenas a la dependencia de servicios de Internet ?		X		SLH25
Las soluciones Web manejan secciones privadas, que se encuentren protegidas por mecanismos de encripción?	X			
Se realizan monitoreos de las actividades realizadas	X			

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LOS SERVICIOS DE INTERNET DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

en los servicios de Internet?				
Los servidores cuenta con contraseñas de acceso?	X			
Existen mecanismos de bloqueo de las maquinas para evitar el acceso al sistema?	X			

EVALUACIÓN SERVICIOS DE INTERNET	**REF:** SLC14 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
ASUNTO	**SI**	**NO**	**N.A**	**R.P.F**
Se realizan actualizaciones relacionadas con seguridad Informática?	X			

EVALUACIÓN A LA SEGURIDAD SERVICIOS DE INTERNET DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH23 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 23	
El proveedor de Internet no presta servicios adicionales frete a la seguridad de la información que se transporta. Evidencia: SLEV23	
RECOMENDACIÓN	
Garantizar que los Servidores y Firewalls se encuentren correctamente configurados, cerrando las entradas que no se estén utilizando.	

EVALUACIÓN A LA SEGURIDAD SERVICIOS DE INTERNET DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH24 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 24	
No existen lineamientos definidos que determinen los procesos de desarrollo para las aplicaciones Web. Evidencia: SLEV24	
RECOMENDACIÓN	
Se recomienda manejar el desarrollo de las aplicaciones de servicios de Internet, según los lineamientos de el modelo de desarrollo de software que mejor se adecue a las necesidades de esta oficina.	

EVALUACIÓN A LA SEGURIDAD SERVICIOS DE INTERNET DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SLH25 **Fecha :** Febrero /2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 25	
No se realiza un seguimiento detallado de las soluciones Web desarrolladas por personas ajenas a la oficina de servicios de Internet, como pasantes, tesis de grado. Evidencia: SLEV25	
RECOMENDACIÓN	
Se recomienda delegar un responsable para realizar un seguimiento a las aplicaciones que se desarrollen para Internet, que verifique las condiciones de seguridad necesarias y la integridad del código.	

SLEV01a

Entrevista Realizada Programador del Centro de Informática
Cuestionario No. 2 (Anexo ANX06)

2. ¿En el documento de aprobación se definen de forma clara los objetivos que se tienen sobre el proyecto?
Si el proyecto es aprobado, entonces, obviamente debe haber unos propósitos y unos objetivos que la oficina se persiga respecto al desarrollo del software o la aplicación, entonces cuando ellos aprueban este proyecto pues nosotros nos fijamos respecto al documento y empezamos a hacer el correspondiente análisis en cuestión de tiempos, para las fases que vamos a hacer, entonces colocamos que si se lo puede terminar en dos meses o tres meses, cuatro meses para la realización del proyecto y en el cual nosotros lo vamos a ejecutar – ¿Esa determinación de tiempos, la realizan ustedes o por parte del Comité de Sistemas les establecen a ustedes las restricciones de tiempo y de recursos que tienen? – No, nosotros porque tenemos el conocimiento y la experiencia, podemos decir cuanto tiempo se demora en hacer un software o un paquete y definimos y acordamos con el jefe de la oficina de informática y que lo vamos a realizar en tal periodo de tiempo – ¿En esos periodos de tiempo están incluidos periodos para revisión del software? – pues si, digamos que si es un periodo cíclico – ¿Qué están haciendo revisiones, pruebas? – Con los usuarios – ¿y se establece una fecha de entrega limite? – diríamos que si se coloca en cuanto a meses, si son tres meses, a veces cuatro cundo pueda estar montado el sistema a no ser que haya inconveniente, algo que no se tenga presupuestado

13. ¿El proceso de análisis se encuentra debidamente o estrictamente documentado?
No – ¿Se hace el proceso de análisis pero no se entra a… digamos a transcribirlo? – Transcribirlo no, porque ellos piden es el software

20. ¿En lo que se refiere a la etapa de diseño, ustedes tienen la documentación, en la que se indique la descripción de interfaces, definición a veces de entidades cuando se refiera al modelo…?
Esta hecha parcialmente, no esta total

43. ¿A los usuarios se les entrega documentación, frente al programa, manuales de usuario, manuales de procedimiento, bosquejos o unas hojas en donde se llega a los procesos?
Ellos toman nota de esos procesos – ¿pero no existe un manual? – No.

SLEV01b

Entrevista realizada a Director del Centro de Informática
Cuestionario No. 1 (Anexo ANX03)

5. ¿Las proyecciones que tiene el centro de informática diseñadas o planteadas a corto, mediano y largo plazo en lo que tiene referencia a la parte lógica, a la parte física y a la parte de recursos humanos, como está diseñada, como está planteada?
.....Nosotros hemos visitado otras universidades y por ponerles un ejemplo la universidad de Pamplona, la oficina de sistemas tiene aproximadamente 25 ingenieros de planta que hacen desarrollo, mantenimiento, soporte técnico, soporte funcional en cuanto a los paquetes que ellos producen, capacitación, es eso aquí realmente hay 2 ingenieros y 2 programadores, para una universidad de pronto mas grande que la de Pamplona, entonces el comité de sistemas se dio cuenta primero el recurso humano, la oficina tiene unas grandes deficiencias, segundo que no hay una organización como dependencia de sistemas por decir algo aquí debería haber ingenieros trabajando en diferentes áreas, por ejemplo debe haber un ingeniero trabajando solo en seguridad, debería haber un ingeniero solo por ejemplo en mantenimiento y soporte a las bases debería haber unos ingenieros como analistas deberían haber unos programadores.....

SLEV02

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2(Anexo ANX06)

14. ¿Participa personal de Auditoría para establecer los controles de seguridad que se deben tener dentro de la aplicación?
Si – ¿Que controles se establecen? – Ellos lo que hacen es una revisión digamos sobre los formatos que se entregan o los reportes, en el caso en estos momentos de matriculas o de contabilidad ellos están periódicamente haciendo revisiones no muy profundas pero si a veces en el funcionamiento del programa por ejemplo en el programa de matriculas que este sacando bien la liquidación, parámetros socio económicos o algunos elementos de reclamos entonces ellos están presentándonos las inquietudes a nosotros o en cierta medida ellos pueden entrar a revisar el software para que se estén entregando los saldos en los balances, si hay una persona sea encargada de esas inquietudes.

Auto Narración

La Oficina de Control Interno, que es la que gestiona la parte de Auditoría no tiene un área especializada en Auditoría de Sistemas que acompañe y controle los procesos de Sistematización de la Universidad. En Control Interno, únicamente se contemplan áreas de Auditoría para la parte financiera y administrativa.

SLEV03

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 3 (Anexo ANX07)

9. ¿La información que ustedes alojan en los bancos de datos se encuentran encriptadas?

Encriptadas no. –¿Y cuando se hace la parte de ingreso ? -Las claves cuando ingresan, si aparecen encriptadas -¿Con mecanismos de encripción del Sistema Operativo?-Del Sistema Operativo.

SLEV04

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2 (Anexo ANX06)

7. ¿El proceso de análisis, el proceso de diseño, el proceso de manejo de base de datos obedece a estándares establecidos dentro de los modelos especificados?

Eso es difícil decirlo por que existe el diseño de base de dato por ejemplo, existen modelos de hace quince años, entonces a veces el cambio puede ser riesgoso hay cosas, hay bases de datos, es que las bases de datos no están unificadas son varias base de datos, debido a que esa bases de datos por ejemplo son muy antiguas, entonces cambian la estructura de ellas y seria cambiar todo el software y el sistema completo cosa que acarrearía un tiempo súper difícil para por ejemplo cambiarlo de una base de datos pues de un diseño antiguo a un diseño normalizado nuevo porque por ejemplo esas bases de datos que hemos encontrado pues están normalizado hasta la segunda forma normal, entonces nosotros quisiéramos en estos momentos cambiarla a la cuarta forma normal, eso implicaría un cambio súper grandísimo y un cambio de todas las aplicaciones entonces, obviamente las aplicaciones nuevas que nosotros hemos construido y nos ha obligado a crear nuevas bases de datos pues las hemos hecho con la metodología que nosotros hemos aprendido o que han aparecido, pero por ejemplo esas aplicaciones viejas no podemos cambiarlas porque acarrearía muchas consecuencias.

SLEV05a

Entrevista realizada a Programador del Centro de Informática

Cuestionario No. 4 (Anexo ANX08)

5. ¿Qué control se maneja para el acceso de usuarios a las aplicaciones?

Como el sistema operativo del Centro es Unix, entonces los diferentes usuarios tienen acceso en las oficinas administrativas que son Contabilidad, Presupuesto, Tesorería, entonces tienen una clave que se hace por aplicativo, es decir hay una para Contabilidad, otra para Presupuesto, otra para Tesorería y Recursos Humanos después del primer acceso adicionalmente cada usuario tiene una clave adicional, que es una clave propia de cada usuario, generalmente viene con su nombre y una clave que ellos mismos han escogido cuando se crea dicho usuario. Las claves entonces, las claves de Contabilidad y presupuesto, entonces no se las cambia nunca pero si la de los usuarios, en cambio que el usuario cambie, entonces el usuario es retirado del sistema y quedan vigentes únicamente las personas que tienen derecho. - ¿Para acceder al sistema maneja contraseña del Sistema Operativo y luego contraseña del aplicativo? - Si, correcto.

8. Me comenta que no realizan cambio de contraseña, entonces, ¿Bajo qué parámetros se realizan cambios de contraseña?

No, únicamente cuando el usuario detecta que alguna persona estuvo a su lado y de pronto logro observar su contraseña, y algunos usuarios que tienen mejores hábitos, ellos hacen que cambie de contraseña mas o menos una vez por mes.

-¿Pero el Procedimiento digamos ellos no lo hacen directamente, sino que hacen la solicitud al Centro de Informática? – Si correcto.

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 1 (Anexo ANX05)

19. ¿Cada cuánto se realiza cambio de contraseñas de los usuarios?
Cada vez que ellos digan, ellos definen eso. – ¿Cada usuario tiene nombre de usuario y contraseña? – Si cada uno tiene su clave, tiene permisos de ejecución

para los programas – ¿Usted asigna los permisos? – Si, digamos que si uno tiene acceso a inventario otro a kardex.

Entrevista realizada a Operario Oficina de Almacén y Compras

(Anexo 12)

5. ¿ Pues en el caso suyo no, pero para las demás, están sugiriendo el cambio de contraseña o ustedes solicitan el cambio de contraseña?

Nosotros cuando hay necesidad si pedimos, pero otra cosa, yo no le puedo poner clave ni nada porque este es el Servidor, entonces, y que tal el Servidor con clave y el día que yo no este no pueden trabaja los otros – ¿esa es la razón? – si esa es la razón.

SLEV05b

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX10)

7. ¿Ustedes realizan cambios periódicos a la clave o es la misma?

Por lo menos trato de hacerlo, frecuentemente cambiar – ¿El programa tiene una opción para realizar el cambio, para que usted pueda realizar el cambio de la clave? – Eso lo hace directamente el administrador del programa – ¿Hay algún mensaje que le sugiera el cambio de contraseña, alguna pantalla? – No, por iniciativa propia.

Entrevista realizada a Operario Oficina de OCARA

(Anexo ANX11)

9. ¿Se realzan cambios de contraseña de manera periódica?

No, en mi caso no, llevo trabajando más de seis años con la misma contraseña.

SLEV06

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX 10)

7. ¿Ustedes realizan cambios periódicos a la clave o es la misma?

Por lo menos trato de hacerlo, frecuentemente cambiar – ¿El programa tiene una opción para realizar el cambio, para que usted pueda realizar el cambio de la clave? – Eso lo hace directamente el administrador del programa – ¿Hay algún mensaje que le sugiera el cambio de contraseña, alguna pantalla? – No, por iniciativa propia.

Entrevista realizada a Operario Oficina de OCARA

(Anexo ANX 11)

12. ¿En algún momento el sistema le esta haciendo mensajes en que sugieran el cambio de contraseña?

No, en mi caso no

SLEV07

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX 10)

7. ¿Ustedes realizan cambios periódicos a la clave o es la misma?

Por lo menos trato de hacerlo, frecuentemente cambiar – ¿El programa tiene una opción para realizar el cambio, para que usted pueda realizar el cambio de la clave? – Eso lo hace directamente el administrador del programa – ¿Hay algún mensaje que le sugiera el cambio de contraseña, alguna pantalla? – No, por iniciativa propia.

Entrevista realizada a Operario Oficina de OCARA

(Anexo ANX 11)

11. ¿Dentro de su menú de usuario existe una opción para el cambio de contraseña?

No, en absoluto

SLEV08

Entrevista realizada a Web Master Universidad de Nariño

(Anexo ANX 09)

8. ¿En cuanto a las aplicaciones que se desarrollan para Internet, qué medidas de seguridad se exigen a los desarrolladores que implemente en el programa?

Se les exige a ver: primero se recibe las aplicaciones sí, realmente exigirles así como unos estándares no hay, pero se los recibe, nosotros les hacemos una serie de pruebas, revisamos pedazos de código – ¿Exactamente qué les revisa? – Sobre todo la parte de autenticación y acceso a ciertas áreas, digamos privadas del sistema, el sistema tiene áreas publicas y privadas, entonces el acceso a esas áreas privadas, tenemos la autenticación como seguridad, en casos donde es necesario utilizar métodos de encripción hay que hacerlo por ejemplo en el sistema de calificaciones hay que hacerlo por ejemplo en el sistema de calificaciones hay que utilizar encripción, hay que utilizar una especie de firma digital. – ¿Se revisa el código de tal manera para verificar que no hayan Caballos de Troya o bombas lógicas? – No, no esa es una de nuestras debilidades. – ¿Básicamente por tiempo, o por qué razón no lo realizan? por tiempo lo que pasa es que hay muchas actividades que realizar acá, y hay muy pocas personas, entonces acá hay que hacer..., hay organizaciones en que hay una persona que se dedica exclusivamente a los servidores, otro a las aplicaciones, otro a la red, y acá solo habemos dos, entonces, es como complicado, no se puede por tiempo y realmente confiamos en la buena fe de los desarrolladores, pero perfectamente nos podrían hacer meternos un Caballo de Troya, uno de esos programas que uno no sabe, de las aplicaciones que le he mencionado en la que soy responsable sí, pero de las otras...también es responsabilidad mía, pero es difícil probar eso.

SLEV09

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2(Anexo ANX06)

14. ¿Participa personal de Auditoría para establecer los controles de seguridad que se deben tener dentro de la aplicación?
Si – ¿Que controles se establecen? – Ellos lo que hacen es una revisión digamos sobre los formatos que se entregan o los reportes, en el caso en estos momentos de matrículas o de contabilidad ellos están periódicamente haciendo revisiones no muy profundas pero si a veces en el funcionamiento del programa por ejemplo en el programa de matriculas que este sacando bien la liquidación, parámetros socio económicos o algunos elementos de reclamos entonces ellos están presentándonos las inquietudes a nosotros o en cierta medida ellos pueden entrar a revisar el software para que se estén entregando los saldos en los balances, si hay una persona sea encargada de esas inquietudes.

Auto Narración

La Oficina de Control Interno, que es la que gestiona la parte de Auditoría no tiene un área especializada en Auditoría de Sistemas que acompañe y cóntrole los procesos de Sistematización de la Universidad. En Control Interno, únicamente se contemplan áreas de Auditoría para la parte financiera y administrativa.

SLEV10

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2 (Anexo ANX06)

34. ¿Los resultados de las pruebas se documentan, por ejemplo aparece un error, se documenta o apareció error en tal parte o se entra a corregir automáticamente?
Nosotros tenemos unas notas, pero son notas individuales de cada funcionario, de cada programador apunta los problemas que encontró y posteriormente procede a corregirlos.

SLEV11

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2 (Anexo ANX06)

40. ¿Las pruebas de aceptación quien las realiza el programador o los usuarios, del funcionamiento ok del programa?
Los usuarios finales dan el visto bueno – ¿Cuándo se hacen las pruebas, se establecen documentos por escrito, por grabación o por algún otro documento en donde se explique, se especifique fecha y hora de la prueba? – Esa circunstancia no, de pronto hay unos oficios de recibido respecto al software que se entrega, que esta en funcionamiento y que de pronto el funcionario puede firmar como recibido o aceptado. – ¿ahí se especifican los procesos que se realizan, las pruebas? – si, diríamos que sí – ¿y en general los programas también? – incluidos los programas, en qué módulos – ¿se documenta también en que equipo se utilizó, se realizan las pruebas? – Si el equipo también.

41. ¿Los usuarios y el director del centro firman un documento en que se apruebe a conformidad las pruebas de aceptación?
En algunos casos si, en el que se presente algún problema que requiera responsabilidad, se hace un oficio en el cual la persona firma de recibido y ha aceptado la modificación que se haga realmente la circunstancia lo amerita.

SLEV12

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2 (Anexo ANX06)

43. ¿A los usuarios se les entrega documentación, frente al programa, manuales de usuario, manuales de procedimiento, bosquejos o unas hojas en donde se llega a los procesos?
Ellos toman nota de esos procesos – ¿pero no existe un manual? – No.

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX10)

9. ¿Usted cuenta con un manual del programa?

No, eso es una falla que tenemos, no tenemos ni de administrador del programa, ni manual del usuario, no hay.

Entrevista realizada a Operario Oficina de Almacén y Compras

(Anexo ANX12)

7. ¿Usted cuenta con un manual de Usuario para el manejo del Programa, les dieron esa información o un manual?

No nosotros por ahí con ellos nos dictaban el curso, luego ellos venían a indicarnos, a enseñarnos como debemos manejar.

Entrevista realizada a Operario Oficina de Contabilidad

(Anexo ANX13)

9. ¿Por parte del Centro de Informática, a ustedes les han facilitado el manual del usuario del programa de manera que los oriente sobre el manejo del mismo?

No, en ningún momento, no tenemos conocimiento.

SLEV13

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2(Anexo ANX06)

-¿En dónde se almacenan las copias de seguridad? – Las tiene Freddy – ¿Quiénes tienen acceso? – Nosotros, las guarda en una gaveta ahí esta echado llave, el tiene la llave

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

13. ¿Cómo se controla el acceso a estas copias?

Bueno simplemente las copias, la persona que este encargada de las copias de seguridad, es quien tiene en su escritorio normalmente, son de fácil acceso realmente. -¿No existe un sitio adecuado para el almacenamiento de cintas? –No, no existe un sitio adecuado.

SLEV14

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

14. ¿Existe algún procedimiento escrito para la restauración de backups?

No, pero la copia como es total del disco duro, entonces es de conocimiento aquí de todos los funcionarios, de que en caso de daño del disco duro, se debe bajar el ciento por ciento de la copia de seguridad, restaurando así el día inmediatamente anterior en su totalidad.

SLEV15

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

15. ¿La información de las backups se encuentra encriptada?

No, no se encuentra encriptada.

SLEV16

Auto Narración

El Comité de Sistemas en el Acta 006 del 5 de marzo de 2003 (Anexo), establece la gestión de la Unidad de Mantenimiento, quienes deberán diligenciar unas fichas en las cuales se identifique las características de los equipos de cada dependencia incluyendo el Software.
Estas fichas serán firmadas por los jefes de cada dependencia en donde también se responsabilicen de no incluir software licenciado.

La Unidad de Mantenimiento realizó esta actividad en el año 2003, a todas las dependencias y Programas de la Universidad de Nariño a excepción del Centro de Informática. Las fichas son almacenadas en la Oficina del Coordinador del Aula, pero no se encuentra el archivo correspondiente a las fichas de las dependencias del Bloque Administrativo.

Se anexa las fichas encontradas de las dependencias de competencia de este trabajo. (Anexo ANX15)

SLEV17

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

6. ¿Se esta actualizando los antivirus?

Si, por Internet se actualizan. – ¿Ustedes están pendientes de las actualizaciones que hacen los proveedores? –Si -¿Mas o menos en que periodo realizan este procedimiento? – Cada tres meses puede ser.

-Manejan algún software que realice control de gusanos, espías o troyanos? – Spydoctor - ¿Se actualiza en lo que se refiere a Parches y otras actualizaciones para el Sistema Operativo? – También, se bajan de Internet las actualizaciones. ¿Quién se encarga de realizarlas directamente las actualizaciones? Freddy – El es el directo encargado? –Si.

SLEV18

Auto Narración

Los funcionarios del Centro de Informática, no tienen ningún tipo de restricción en cuanto descargas por Internet, ellos utilizan este servicio para bajar programas para labores de tipo técnico.

SLEV19

Auto Narración

El Centro de Informática no cuenta con la Licencia correspondiente del Sistema Operativo en uso Unix 5.05., cuenta con la licencia de Unix 3.2 – 4.2 La cual se dejo de usar por las nuevas necesidades de procesamiento que exigía los procesos de la Universidad. Unix versión 5.05 fue concedido a la Universidad de Nariño por Corponariño siendo que la última institución no la tenía en uso y para la Universidad era una necesidad. Entonces se fijo realizar un convenio entre las dos instituciones, pero nunca se concretó nada por parte de las directivas, y es así como hoy la Universidad no cuenta con la licencia del Sistema Operativo.

Observar Relación de Licencias de la Universidad de Nariño establecida por el Aula de Informática. (Anexo ANX16)

SLEV20

Auto Narración

En conversación informal con funcionarios del Centro de Informática, se establece que la información que manejan los Sistemas de la Universidad de Nariño, pese a su importancia y delicadeza no utiliza ningún mecanismo de encriptación.

SLEV21

Auto Narración

Los funcionarios de Centro de Informática, realizan a diario procedimientos de backups, algunos a medio día y seis de la tarde, automáticamente se realizan copias de todos los sistemas a las diez de la noche, es de conocimiento de los funcionarios el procedimiento de backups y siendo concientes de la importancia son muy puntuales y responsables con este hecho. Sin embargo, en el Centro de Informática no existe un documento que señale los pasos a seguir para realizar backups. Este documento serviría para establecer el cumplimiento de realización de copias de respaldo y para funcionarios nuevos informarían del proceso que deben seguir.

SLEV22

Entrevista realizada a Programador del Centro de Informática
Cuestionario No.2 (Anexo ANX06)

25. ¿Los programas poseen internamente sus propios procedimientos, que permitan recuperar información en el caso de un fallo, por ejemplo del sistema, digamos sabemos por ejemplo hay ciertos programas que en el momento que haya una caída de luz, se borran, se pierden las relaciones, cierto hay algún proceso interno de los programas que permita recuperar o hacer restauración de archivo?
Tenemos rutinas en cuanto en la base de datos que reparan las tablas o que reconstruyen los índices o que sacan copias en archivos planos en el caso de esta base de datos, es recursivo todo – ¿Me imagino que manejen controles, para identificar y corregir los datos? – Si
.

SLEV23

Entrevista realizada a WebMaster Universidad de Nariño

Cuestionario No. 5 (Anexo ANX09)

5. ¿Quién es el proveedor de Internet?
Telecom.

6. ¿Qué servicios de seguridad les ofrecen ellos para Internet?
Ninguno el proveedor nos entrega un canal limpio de datos a Internet, la seguridad y la protección esta a cargo del cliente.

SLEV24

Entrevista realizada a WebMaster Universidad de Nariño
Cuestionario No. 5 (Anexo ANX09)

8. ¿En cuanto a las aplicaciones que se desarrollan para Internet, qué medidas de seguridad se exigen a los desarrolladores que implemente en el programa?

Se les exige haber, primero se recibe las aplicaciones sí, realmente exigirles así como unos estándares no hay, pero se los recibe, nosotros les hacemos una serie de pruebas, revisamos pedazos de código – ¿Exactamente qué les revisa? – Sobre todo la parte de autenticación y acceso a ciertas áreas, digamos privadas del sistema, el sistema tiene áreas publicas y privadas, entonces el acceso a esas áreas privadas, tenemos la autenticación como seguridad, en casos donde es necesario utilizar métodos de encripción hay que hacerlo por ejemplo en el sistema de calificaciones hay que hacerlo por ejemplo en el sistema de calificaciones hay que utilizar encripción, hay que utilizar una especie de firma digital. .....

SLEV25

Entrevista realizada a WebMaster Universidad de Nariño
Cuestionario No. 5 (Anexo ANX09)

8. ¿En cuanto a las aplicaciones que se desarrollan para Internet, qué medidas de seguridad se exigen a los desarrolladores que implemente en el programa?

Se les exige, primero se recibe las aplicaciones sí, realmente exigirles así como unos estándares no hay, pero se los recibe, nosotros les hacemos una serie de pruebas, revisamos pedazos de código – ¿Exactamente qué les revisa? – Sobre todo la parte de autenticación y acceso a ciertas áreas, digamos privadas del sistema, el sistema tiene áreas públicas y privadas, entonces el acceso a esas áreas privadas, tenemos la autenticación como seguridad, en casos donde es necesario utilizar métodos de encripción hay que hacerlo por ejemplo en el sistema de calificaciones hay que hacerlo por ejemplo en el sistema de calificaciones hay que utilizar encripción, hay que utilizar una especie de firma digital. – ¿Se revisa el código de tal manera para verificar que no hayan Caballos de Troya o bombas lógicas? – No, no esa es una de nuestras debilidades. – ¿Básicamente por tiempo, o por qué razón no lo realizan? por tiempo lo que pasa es que hay muchas actividades que realizar acá, y hay muy pocas personas, entonces acá hay que hacer..., hay organizaciones en que hay una persona que se dedica exclusivamente a los servidores, otro a las aplicaciones, otro a la red, y acá solo habemos dos, entonces, es como complicado, no se puede por tiempo y realmente confiamos en la buena fe de los desarrolladores, pero perfectamente nos podrían hacer meternos un Caballo de Troya, uno de esos programas que uno no sabe, de las aplicaciones que le he mencionado en la que soy responsable sí, pero de las otras...también es responsabilidad mía, pero es difícil probar eso.

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD AL PERSONAL DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Verificar que los usuarios tengan una adecuada capacitación en el manejo de los programas, para no incurrir en errores por falta de conocimiento.

EVALUACIÓN DE LA CAPACITACIÓN DE PERSONAL	**REF:** SPC01 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Capacitación				
Los usuarios reciben capacitación necesaria para el manejo de los programas, por parte del personal del Centro de Informática?		X		SPH01
Cuenta con un manual de usuario que le oriente en el manejo de sistema?		X		SPH02
Es claro y objetivo el manual del usuario?			X	
Que opinión tiene del manual?			X	
Manual de Funciones y Procedimientos				
Se cuenta con un manual de funciones que especifique claramente las responsabilidades del funcionario?	X			
Se conoce claramente el manual de funciones?		X		SPH03
El manual es acorde a las responsabilidades de los funcionarios?		X		SPH03
Existe Manual de Procedimientos, para los funcionarios del Centro de Informática?		X		SPH04

EVALUACIÓN A LA CAPACITACIÓN DE LOS USUARIOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH01 **Fecha :** JUNIO/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 01	
Muchos usuarios de las dependencias, no han recibido una capacitación que satisfaga sus necesidades en el manejo del aplicativo. Cuando se trata de funcionarios nuevos, son los otros funcionarios de la dependencia quienes se encargan de asesorar en el manejo del programa, Para resolver sus inquietudes tienen que llamar en repetidas ocasiones a los funcionarios del Centro de Informática. Evidencia: SPEV01	
RECOMENDACIÓN	
Programar ciclos de capacitación en el manejo de los programas que son de responsabilidad del Centro de informática, y aprovechar esos espacios para retroalimentar la aplicación.	

EVALUACIÓN A LA CAPACITACIÓN DE LOS USUARIOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH02 **Fecha :** JUNIO/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 02	
No se entrega Manual de Usuario de los programas que desarrolla el Centro de Informática, esto hace que los usuarios no tengan una guía para orientarse en el manejo de los programas. Evidencia: SPEV02	
RECOMENDACIÓN	
El director del proyecto de desarrollo de software o el director del Centro de Informática, debe garantizar la creación y entrega del Manual de Usuario final, el cual debe estar escrito en un lenguaje no técnico, debe ser de fácil entendimiento y debe permitirle a un usuario que después de la lectura del manual pueda realizar un manejo adecuado del software.	

EVALUACIÓN A LA CAPACITACIÓN DE LOS USUARIOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH03 **Fecha :** JUNIO/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 03

Los funcionarios no tienen conocimiento del Manual de Funciones de su cargo.

Este Manual no contempla verdaderamente las funciones de la naturaleza de los cargos existentes.

Evidencia: SPEV03

RECOMENDACIÓN

Actualizar el Manual de Funciones de la Universidad de Nariño, de acuerdo con las actividades y funciones que realmente cumplen los funcionarios y acorde a los cargos existentes, posterior a esto, entregar el Manual de Funciones a los funcionarios que especifique claramente las actividades propias de su cargo.
Es fundamental que los funcionarios conozcan este Manual.

EVALUACIÓN A LA CAPACITACIÓN DE LOS USUARIOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH04 **Fecha :** JUNIO/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 04	
No existe Manual de Procedimientos para los funcionarios del Centro de Informática. Evidencia: SPEV04	
RECOMENDACIÓN	
Realizar por parte de la Oficina de Planeación el Manual de Procedimientos que corresponde para el Centro de Informática, contando con la participación del Director o un delegado. Entregar una copia del Manual de Procedimientos a los funcionarios.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DE LA ERGOMETRÍA Y BIENESTAR LABORAL

OBJETIVO

Evaluar la forma como interactúan los usuarios en el entorno informático, de tal manera, que no se ocasionen lesiones musculares, visuales, auditivos y mentales.

EVALUACIÓN DE LA ERGOMETRÍA Y BIENESTAR LABORAL **CENTRO DE INFORMÁTICA (C.I.)**	**REF:** SPC02 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
La distribución de los dispositivos del computador facilita una posición natural del usuario?	X			
El puesto de trabajo facilita su adecuación para que el usuario se coloque en posición cómoda y a su medida?	X			
La definición del monitor es la adecuada para no forzar la vista?	X			
Los monitores tienen protectores de pantalla?		X		SPH05
Están exentos los funcionarios de efectos de estrés ocasionados por la carga excesiva de trabajo?		X		SPH06
Cuenta el Centro de Informática con una iluminación suficiente y adecuada?	X			

Están los sitios de trabajo de los funcionaros libres de equipos altamente ruidosos?	X			
Existe una adecuada ventilación en el área de trabajo	X			

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH05 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 05	
Los computadores del Centro de Informática no están provistos de protectores de pantalla, pudiendo ocasionar a los operadores trastornos visuales al estar expuestos por tiempo prolongado a la pantalla del computador. Evidencia**:** SPEV05	
RECOMENDACIÓN	
Disponer de protectores de pantalla para los computadores del Centro de Informática o por parte de los operarios hacer que utilicen anteojos con protección para el monitor.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH06 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 06	
Los trabajadores del Centro de Informática, tienen excesiva carga de trabajo que pueden ocasionar problemas de estrés que afecten en el desempeño de sus actividades laborales. Evidencia: SPEV06	

RECOMENDACIÓN
Realizar un estudio de la demanda de servicios que realiza el Centro de Informática, con el fin de determinar la capacidad operativa frente al tiempo de respuesta que deben presentar los trabajadores para dar cumplimiento eficiente de sus responsabilidades.

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DEL CONTROL DE ACCESO

OBJETIVO

Evaluar las medidas de aseguramiento para impedir el acceso no autorizado, de manera que eviten riesgos potenciales de ataque, pérdida, robo o daño a los equipos y periféricos

EVALUACIÓN DEL C0NTROL DE ACCESO A LAS INSTALACIONES DEL CENTRO DE INFORMÁTICA (C.I)	**REF:** SPC03 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**

Ingreso de Personas				
El acceso al C.I. esta restringido únicamente a personal autorizado?	X			
Existe sistema electrónico de control de acceso?		X		SPH07
Existe un responsable del control de accesos?	X			
El personal del C.I. porta permanentemente y de forma visible un carnét de identificación?		X		SPH08
El control de acceso se realiza a la entrada al CI?	X			
Se tiene un control permanente de acceso anotando: Nombre del visitante autorizado? Nombre de quien autoriza? Motivo? Fecha, hora de acceso y firma? Fecha , hora de salida y firma?		 X X X X X		SPH09
Estas listas se guardan al menos por un año?			X	
Se tienen establecidos horarios de acceso a las instalaciones?	X			
El acceso a personal fuera de la jornada laboral es autorizado por el director o el responsable?	X			

EVALUACIÓN DEL C0NTROL DE ACCESO **A LAS INSTALACIONES** **DEL CENTRO DE INFORMÁTICA (C.I)**	**REF:** SPC04 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
ASUNTO	**S**	**N**	**N.A**	**R.P.F**
El personal ajeno se identifica con un carné de visitante?		X		SPH10
El acceso a personas ajenas al Centro de Informática es autorizado por el director o por el responsable de accesos?	X			
Se toman las medidas de seguridad adecuadas después que los empleados han terminado sus contratos de trabajo?	X			

Existe un responsable de la llave, de la puerta de acceso?	X			
Existe un responsable de la llave, del cuarto de máquinas?	X			
Existe algún dispositivo electrónico detector de intrusos?		X		SPH11
Vigilancia				
Existe servicio de vigilancia en el perímetro de las instalaciones?	X			
El personal de vigilancia en las noches realiza rondas de por lo menos cada 10 minutos?		X		SPH12
Se capacita a estas personas sobre las medidas a tomar en caso de que alguien quiera entrar sin autorización?		X		SPH13
Se evalúa al personal de vigilancia antes de ser contratado?	X			

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :**SPH07 **Fecha :** Abril /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 07	
El Centro de Informática no dispone de un sistema electrónico para realizar control de acceso. Evidencia: SPEV07	
RECOMENDACIÓN	
Instalar en la puerta de acceso al área operativa y en la puerta de acceso al cuarto de máquinas un sistema electrónico de control de acceso como: lector de banda magnética o un sistema de clave electrónica. Este sistema debe hacer un registro que indique: identificación de la persona, fecha y hora de ingreso como también fecha y hora de salida, observaciones en caso que sea necesario.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH08 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 08	
El personal de la oficina del Centro de Informática, no porta un carné que los identifique como funcionarios de esta dependencia. Evidencia: SPEV08	
RECOMENDACIÓN	
Identificar al personal de la oficina del Centro de Informática, portando de manera visible y permanente un carné, que indique: nombre, documento de identificación, cargo y dependencia a la cual pertenece el funcionario. Esta medida, facilita su identificación para el proceso de control de acceso.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH09 **Fecha :** Abril /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 09	
No se tiene establecido un control escrito a la entrada del Centro de Informática, que registre el acceso de personas autorizadas y visitantes al Centro de Informática. Evidencia: SPEV09	

RECOMENDACIÓN
Establecer un control de acceso a la entrada del Centro de Informática, registrando en una lista nombre de la persona que ingresa, fecha, hora de entrada y salida; si es personal ajeno al Centro de Informática señalar motivo y la persona que lo autoriza. Guardar estas listas en un lugar seguro para posteriores revisiones. Si no es posible establecer esta medida de control en el Centro de Informática, situar a la entrada del edificio un vigilante, que controle el acceso de personas, de manera que el personal autorizado ingrese con el carné que lo identifica como funcionario de la Universidad, el personal ajeno a la institución deberá entregar un documento de identificación y se le otorgará carné de visitante. Se recomienda instalar una cámara de video que capte el movimiento a la entrada del edificio. Para optimizar el proceso de control de acceso, se recomienda que el ingreso de personas que se dirigen a caja, ubicada en la oficina de Tesorería, realicen el ingreso por la puerta trasera de esta oficina.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH10 **Fecha :** Agosto/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 10	
El personal ajeno a la institución, que ingresa a la oficina del Centro de Informática, no porta un carné que los identifique como visitantes.	

Evidencia: SPEV08
RECOMENDACIÓN
El vigilante encargado del control de acceso de personas al bloque administrativo, debe solicitar al personal que no pertenece a la Universidad de Nariño, algún tipo de documento de identificación, a cambio del cual le otorgara un carné que los identifique en función de visitantes, para ingresar a las instalaciones del Bloque Administrativo, en horarios de atención.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH11 **Fecha :** Abril /2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 11

El Centro de Informática, no posee un sistema electrónico detector de intrusos que alerte al personal de vigilancia en casos de intrusión.

Evidencia: SPEV10

RECOMENDACIÓN

Instalar en la puerta y ventanas del Centro de Informática, un sistema electrónico de detección de intrusos conectados a una alarma, que alerte al personal de vigilancia encargado de la seguridad del edificio, en el momento que se trate de hacer la intrusión.
Los detectores que se pueden instalar son:

- Detector de aberturas
- Detector de roturas de vidrio
- Detector de vibraciones que detecta golpes o manipulaciones extrañas sobre la superficie controlada.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH12 **Fecha :** Abril /2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 12

El edifico donde se localiza el Centro de Informática, dispone de un sólo vigilante que cubre las áreas del bloque Administrativo, Biblioteca, Auditorio, Bloque 2 y Bloque 3, siendo esta un área muy amplia para tener un eficiente control sobre toda ella . En las noches no existe un control sobre las rondas que realizan los vigilantes, realizándolas ellos en periodos de tiempo demasiado extensos, con lo cual da tiempo suficiente para que personas mal intencionadas puedan realizar actos delictivos o ingresar forzosamente a esta dependencia, sin ser detectados a tiempo por los vigilantes.

Evidencia: SPEV11

RECOMENDACIÓN

Reforzar el sistema de vigilancia, con un vigilante exclusivo para el bloque Administrativo que es donde se localiza esta dependencia y establecer controles de tiempo para las rondas nocturnas del personal de vigilancia a cargo.

Dotar al Centro de Informática, de un sistema electrónico para detección de intrusos, al cual reaccione el personal de vigilancia.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SPH13 **Fecha :** Abril /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 13	
El personal de vigilancia, no está capacitado en cuanto al manejo de situaciones en caso, que alguien quiera ingresar por la fuerza, a las instalaciones del bloque administrativo, con lo cual se corre el riesgo de incurrir en accidentes o problemas de pérdida de vidas.	

Evidencia: SPEV12
RECOMENDACIÓN
Capacitar al personal de vigilancia de la Universidad de Nariño, en lo referente a procedimientos, frente a posibles casos de accesos no autorizados o actos delictivos, para que adopten medidas de protección, cuidando la vida de las personas.

SPEV01

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX10)

8. ¿Frente a la capacitación, a usted le han dado la capacitación necesaria para el manejo del programa?
De todas maneras, no, de pronto se me facilita un poco porque tengo una tecnología en administración Informática y soy técnico en sistemas, por eso se me facilita un poco pero así que se hayan sentado a decirme esto, esto, no, si no que ya por la misma experiencia, pero realmente si se hace necesario, no solamente la parte operativa si no de manejar lo más eficiente el programa

Entrevista realizada a Operario Oficina de OCARA

(Anexo ANX11)

4. ¿En lo que se refiere al desarrollo del software, hay disponibilidad por parte del Centro de Informática para atender sus necesidades e inquietudes, acerca de la aplicación que manejan?

El centro de Informática es una dependencia de la Universidad que maneja muchas cosas y por el volumen de actividades que realizan, en su momento cuando se le presentan problemas a uno, no se lo solucionan de ya, si no lo dejan, esperemos para mañana o te mandamos a un monitor del aula, cuando son cosas demasiadamente urgentes, entonces toca que estar llame y llame, pero de pronto no es porque la entidad o la dependencia no pueda arreglarlos, es por el innumerable número de actividades que ellos realizan, que el personal no es suficiente para atender las necesidades que nosotros desarrollamos o que tenemos.

Entrevista realizada a Operario Oficina de Contabilidad

(Anexo ANX13)

8. ¿Referente a la capacitación que ustedes han tenido para el manejo del programa, considera que ha sido suficiente la capacitación por parte del Centro de Informática?
Pues hemos recibido las especificaciones correspondientes para el manejo, sin embargo no tenemos una amplitud cuando uno quiere ya salirse o necesita salirse de los parámetros, estamos como muy limitados, entonces ya nos toca acudir a ellos y en ocasiones que el compañero no esté y que este prestando atención en otra dependencia, uno tiene que esperarlo hasta que llegue, entonces, yo creo que nos hace falta como un poquito más de flexibilidad, que uno pueda tener mas entrada al sistema, que pueda, cualquier cosita que yo necesito, cambiar un listado, sacarlo aquí, sacarlo acá o hacer una corrección de pronto… hacerlo más directamente

SPEV02

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 2(Anexo ANX06)

43. ¿A los usuarios se les entrega documentación, frente al programa, manuales de usuario, manuales de procedimiento, bosquejos o unas hojas en donde se llega a los procesos?
Ellos toman nota de esos procesos – ¿pero no existe un manual? – No.

Entrevista realizada a Operario Oficina de Tesorería

(Anexo ANX10)

9. ¿Usted cuenta con un manual del programa?

No, eso es una falla que tenemos, no tenemos ni de administrador del programa, ni manual del usuario, no hay.

Entrevista realizada a Operario Oficina de Almacén y Compras

(Anexo ANX12)

7. ¿Usted cuenta con un manual de Usuario para el manejo del Programa,

les dieron esa información o un manual?

No nosotros por ahí con ellos nos dictaban el curso, luego ellos venían a indicarnos, a enseñarnos como debemos manejar.

Entrevista realizada a Operario Oficina de Contabilidad

(Anexo ANX13)

9. ¿Por parte del Centro de Informática, a ustedes les han facilitado el manual del usuario del programa de manera que los oriente sobre el manejo del mismo?

No, en ningún momento, no tenemos conocimiento.

SPEV03

Entrevista realizada a Programador del Centro de Informática
Cuestionario No. 1 (Anexo ANX06)

1. ¿Las funciones que Usted realiza dentro del Centro de Informática, corresponden a las establecidas en el manual de funciones de la Universidad de Nariño?

Sí, es correcto respecto lo que aparece acá respecto al análisis de requisitos, la creación de programas y también los mantenimientos que se le hacen al sistema operativo están incluidos acá. – ¿Adicional a las funciones que están ahí realiza

otras funciones, le corresponderían funciones como las del analista? – Si es casi, estaríamos mezclando las dos. – ¿usted tenia conocimiento de estos manuales? – No – ¿Ni entre lo oficial y no oficial? – No.

Entrevista realizada a Director del Centro de Informática
Cuestionario No. 1 (Anexo ANX03)

8. ¿Usted por que cree que existe esa discordancia entre lo que dice el manual de funciones de la universidad y lo que realmente es?
Yo realmente no voy a echarle la culpa a nadie pero me parece que quienes levantaron este manual no tuvieron en cuenta la resolución que crea el comité de sistemas asignándole las funciones entonces realmente hay unas funciones que son del comité de sistemas que el comité las hace a manera de propuestas o políticas pero quien ejecutaría algunas de esas políticas es el director.
Dirigir, supervisar y promover y participar en los estudios que permitan mejorar la prestación de los servicios de la dependencia, esta bien, yo la resumiría en dar cumplimiento a las disposiciones del comité de sistemas en cuanto investigaciones que permitan mejorar la prestación de servicios de la dependencia.

SPEV04

Auto Narración

La Oficina de Planeación cuenta con Manuales de Procedimientos del año 1999, para las dependencias de Contabilidad y Presupuesto, Almacén y Compras y otras dependencias de la Universidad. No figura Manual de Procedimientos para el Centro de Informática.

En la solicitud de esta documentación nos dimos cuenta que las dependencias para las cuales existe el Manual de Procedimientos, no saben de la existencia del mismo, puesto que la oficina de Planeación no lo ha dado a conocer.

SPEV05

EQUIPOS SIN PROTECTOR DE PANTALLA
CENTRO DE INFORMÁTICA

SPEV06

Auto Narración

Los funcionarios del Centro de Informática, tienen que cumplir con muchas actividades y estrictamente en periodos de tiempo cortos debido a la exigencia y necesidad de las mismas, y siendo el número de personal reducido para cumplir con todas las actividades del Centro de Informática, hace que el personal existente se recargue de trabajo, tensionándose y pudiendo ocasionar daños de estrés en la persona que afecten el desempeño de sus funciones.

SPEV07

INGRESO ÁREA DE PROGRAMACIÓN
SIN CONTROL DE ACCESO ELECTRÓNICO
CENTRO DE INFORMÁTICA

CUARTO DE MÁQUINAS
SIN CONTROL DE ACCESO ELECTRÓNICO
CENTRO DE INFORMÁTICA

SPEV08

Auto Narración

En el Centro de Informática y en general en la Universidad de Nariño no se utiliza carné de identificación que distinga a los funcionarios que trabajen en una determinada dependencia. Existe la medida de carné de visitante el cual se otorga a la entrada de la Universidad, mas sin embargo este control casi nunca se realiza y tampoco se realiza de una manera óptima que realmente garantice la seguridad se acceso, debido a que no es una medida que se aplique con todas las personas y de manera constante. Además contando que la Universidad tiene dos puertas de acceso y esta medida solo se establece en una.

SPEV09

Auto Narración

En ninguna de las dependencias de la Universidad de Nariño se lleva un control escrito de la entrada y salida de personas tanto funcionarios de la misma dependencia, al igual que personal de visita que se encuentre autorizado.
Esta medida podría realizarse no necesariamente a la entrada del Centro de Informática sino a la entrada del Bloque Administrativo, estableciendo así control sobre las otras dependencias y sabiendo que existe una persona designada en la entrada del edificio, la cual podría realizar perfectamente este procedimiento de control.

SPEV10

PUERTA Y VENTANA PUNTO MAS VULNERABLE DE INGRESO DEL CENTRO DE INFORMÁTICA NO POSEE SISTEMA DETECTOR DE INTRUSOS

SPEV11

Auto Narración

En noches en las cuales estuvimos pendientes del procedimiento de vigilancia nocturnas, pudimos observar que el área que cubre el vigilante es demasiado grande par tener control sobre ella, así el vigilante cuando cierra el bloque administrativo aproximadamente 7:00 pm, va a dar la ronda por los otros bloques y deja espacios de mas de media hora sin ir a revisar el Bloque administrativo, inclusive en alguna ocasión miramos al vigilante barriendo, función que no le corresponde y lo descentraliza de su trabajo.

SPEV12

Auto Narración

Cuando se le preguntó a uno de los vigilantes del bloque administrativo, en conversación informal, qué haría en caso de alguien quisiera realizar un ingreso forzoso al Bloque administrativo, y el respondió: “echar bala”, consultando a una empresa de vigilancia sobre este caso, argumentan que en la capacitación a un vigilante la última medida es la utilización de armas ya que ante todo se debe preservar la vida

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DE LA UBICACIÓN Y CONSTRUCCIÓN

OBJETIVO

Evaluar las condiciones de las instalaciones en lo referente a construcción y ubicación de manera que garanticen la protección de los recursos informáticos que se encuentran dentro de ésta.

EVALUACIÓN DE LA UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE INFORMÁTICA	**REF:** SFC01 **Elaboró:** M.C.T y E.A.F **Fecha :** Marzo / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Ubicación				
Se encuentra el Centro de Informática ubicado en una zona libre de alto tráfico de personas?	X			
Está localizado el Centro De Informática en un lugar distante de la calle?	X			
El Centro De Informática se ubica en un área interna de la Universidad?	X			

Se encuentra el Centro de Informática distante de elementos peligrosos o combustibles?	X			
El Centro de Informática esta fuera de la influencia de señales de radar?	X			
El piso en que se encuentra el Centro de Informática: -Dificulta el acceso por la parte externa del edificio? -Facilita la entrada de bomberos y procesos de evacuación? -Es menos propenso a las inundaciones?	X X	X		SFH01
La tubería de agua se encuentra retirada del área del Centro de Informática.?	X			
EVALUACIÓN DE LA UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE INFORMÁTICA	**REF:** SFC02 **Elaboró:** M.C.T y E.A.F **Fecha :** Marzo / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
La orientación del Centro de Informática está libre de exposición constante al sol?	X			
La ubicación del Centro de Informática es cercana a las dependencias a las cuales presta servicio? - OCARA - Almacén y Compras - Contabilidad y Presupuesto - Recursos Humanos - Tesorería y Pagaduría - Control Interno	X X	X X		SFH02

Diseño				
Para la construcción del edifico donde se localiza el Centro de Informática, se consultó al director para establecer la distribución de espacios, disposición de la red de datos y red eléctrica?	X			
Fueron atendidos los requerimientos del director?		X		SFH03
Existen los planos arquitectónicos del Bloque Administrativo?	X			
Existen los planos arquitectónicos de la división de áreas del Centro de Informática?		X		SFH04
Existen los planos de la red eléctrica?		X		SFH05
Existen los planos de la red de datos?		X		SFH06
Paredes				
El material de las paredes principales es incombustible?	X			
El material de las paredes principales es antiestático?	X			
Las paredes internas principales son suficientemente rígidas para sostener los equipos?	X			
Las paredes se encuentran perfectamente selladas para evitar la entrada de polvo?	X			
Las paredes están exentas de fisuras?	X			
EVALUACIÓN DE LA **UBICACIÓN Y CONSTRUCCIÓN** **DEL CENTRO DE INFORMÁTICA**	**REF:** SFC03 **Elaboró:** M.C.T y E.A.F **Fecha :** Marzo / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
La pintura de las paredes del Centro de Informática es: -Incombustible? -Lavables? -De color claro?	 X X X			

El material de las divisiones es de material incombustible?		X		SFH07
El material de las divisiones es antiestático?		X		SFH08
Pisos y Cielo Raso				
El material del piso es: - Incombustible? - Antiestático? - Impermeable? - Antideslizante?	 X X X X			
El material del cielo raso es: - Incombustible? - Antiestático? - Impermeable?	 X X X			
Puertas				
La puerta de acceso se encuentra en el interior del edificio?	X			
La puerta de acceso principal al Centro de Informática es de abertura completa?	X			
La puerta principal del Centro de Informática es de material incombustible?	X			
Está la puerta principal de acceso protegida de accesos forzosos?		X		SFH09
La puerta abre al ras sin dejar espacio por debajo?	X			
La puerta esta provista de algún dispositivo electrónico, para detección de intrusos?		X		SFH10

EVALUACIÓN DE LA **UBICACIÓN Y CONSTRUCCIÓN** **DEL CENTRO DE INFORMÁTICA**	**REF:** SFC04 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Tiene por lo menos una chapa de seguridad?	X			
La chapa es resistente a intentos de violación?		X		SFH11
Las puertas internas son incombustibles?		X		SFH07
Ventanas				
Las ventanas están protegidas de la entrada de excesiva luz solar?	X			
Las ventanas exteriores están protegidas con antepecho de hierro ?	X			
Las ventanas internas están protegidas con antepecho de hierro ?		X		SFH09
Las ventanas cierran completamente?	X			
Los vidrios de las ventanas son de seguridad ?		X		SFH09
El sellamiento de los vidrios es compacto?		X		SFH12
Las ventanas poseen algún mecanismo detector de intrusos?		X		SFH10
Distribución De Áreas				
El espacio del Centro de Informática esta considerado para el incremento de equipos y de personal?		X		SFH13
Existe un espacio aislado exclusivo para el almacenamiento de papelería?		X		SFH14
Se encuentra previsto un espacio adecuado para el almacenamiento de equipos?		X		SFH14
Se encuentra establecida un área para el mantenimiento de equipos?		X		SFH15
Se tiene prevista un área de programación?	X			

Se provee de un lugar protegido para almacenamiento de discos, cintas?	X			
Se tiene un área exclusiva para equipo de protección eléctrica?	X			
EVALUACIÓN DE LA **UBICACIÓN Y CONSTRUCCIÓN** **DEL CENTRO DE INFORMÁTICA**	**REF:** SFC05 **Elaboró:** M.C.T y E.A.F **Fecha :** Marzo / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Existen suficientes números de cubículos?	X			
Existe una adecuada área de atención al publico?		X		SFH16

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH01 **Fecha :** Marzo / 2004 **Elaboro:** E.A.F. y M.C.T.

HALLAZGO 01

El Centro de Informática de la Universidad de Nariño, se ubica en el primer piso del Bloque Administrativo, con ventanas que comunican al exterior del edificio. Estas características hacen al Centro de Informática vulnerable en cuanto a acceso físicos forzosos y/o objetos que puedan causar daños o pérdida de los equipos que aquí se encuentran.

Evidencia: SFEV01

RECOMENDACIÓN

Se recomienda que el Centro de Informática, se ubique en un segundo piso, libre de alto tráfico de personas y en la medida de lo posible evitar ventanas hacia la parte externa de la edificación.

Como medida de protección a la situación actual del Centro de Informática, se recomienda utilizar vidrios de seguridad.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH02 **Fecha :** Marzo / 2004 **Elaboro:** E.A.F. y M.C.T.
HALLAZGO 02	
El Centro de Informática de la Universidad de Nariño, se encuentra distante de la dependencia de Almacén y Compras y de la dependencia de OCARA. **Evidencia: SFEV02**	
RECOMENDACIÓN	
Se recomienda que el Centro de Informática, se ubique de manera estratégica y cercana a las dependencias a las cuales presta el servicio dentro de las instalaciones de la Universidad, permitiendo óptima instalación del cableado y respuestas rápidas ante problemas.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH03 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 03	
El diseño y distribución de espacios del Centro de Informática se realizó teniendo en cuenta el personal y equipos existentes hasta el momento, no se considero el incremento de los mismos y el espacio suficiente para disponer de una cintoteca y discoteca además que almacenamiento de papelería y equipos. **Evidencia: SFEV03 - SFEV04**	

RECOMENDACIÓN
Permitir que el personal del Centro de Informática, en particular el director, participe de forma activa en eventuales construcciones o diseño para el Centro de Informática para definir la distribución de espacios de esta dependencia, así como el diseño de la red de datos y red eléctrica. Se recomienda que el director revise los planos arquitectónicos y emita su aprobación. La construcción del Centro de Informática y su distribución debe contemplar una proyección de crecimiento por lo menos a 10 años, tanto en equipos como en personal. La distribución de espacios debe tener en cuenta: • Oficina del Director. • Oficina de secretaria. • Espacios para personal operativo. • Espacios para atención del público. • Espacio para servidores. • Espacio para equipos de protección. • Espacios de archivos y almacenamiento de papel, discos y cintas.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH04 **Fecha :** Marzo /2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 04
En el Centro de Informática y en la oficina de planeación, no existen los planos arquitectónicos del Centro de Informática y tampoco de las dependencias a las cuales presta servicio. **Evidencia: SFEV05-SFEV06**
RECOMENDACIÓN
Realizar un levantamiento de planos de las áreas del Centro de Informática y de las dependencias, a las cuales presta el servicio. Para futuras construcciones se debe garantizar que el equipo constructor, deje los planos en la oficina de Planeación y sacar copia para el Centro de Informática.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH05 **Fecha :** Marzo /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 05	
No existen los planos de la red de datos instalada en el Centro de Informática. **Evidencia: SFEV05**	
RECOMENDACIÓN	
Realizar el levantamiento de planos de la red de datos del Centro de Informática y de las dependencias a las cuales presta el servicio.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH06 **Fecha :** Marzo /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 06	
No existen los planos de la red eléctrica instalada en el Centro de Informática. **Evidencia: SFEV05**	
RECOMENDACIÓN	
Realizar el levantamiento de planos de la red eléctrica del Centro de Informática y de las dependencias a las cuales presta el servicio.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH07 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 07	
Las divisiones internas del Centro de Informática, al igual que muebles, papeleras y puertas son de material combustible, estos elementos facilitan la propagación del fuego en caso de presentarse un incendio. **Evidencia: SFEV07**	
RECOMENDACIÓN	
Evitar dentro del Centro de Informática elementos de fácil combustión y remplazarlos por objetos de material incombustible.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH08 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 08	
Las divisiones internas del Centro de Informática son de material antiestático, que podrían producir descargas y afectar los dispositivos de hardware que aquí se encuentran. **Evidencia: SFEV08**	
RECOMENDACIÓN	
Mantener tapados los equipos del Centro de Informática. Disponer de un sitio libre de elementos antiestáticos para almacenar los dispositivos de hardware y realizar mantenimiento de los equipos. Evitar la utilización de materiales antiestáticos en el entorno de trabajo del Centro de Informática.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH09 **Fecha :** Marzo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 09	
La ventana interna y la puerta de acceso principal a la dependencia del Centro de Informática, no están protegidas con antepecho de hierro y tampoco poseen vidrios de seguridad blindados, convirtiéndose en un elemento vulnerable para el ingreso no autorizado de personas, puesto que el vidrio se rompe con facilidad dejando suficiente espacio para poder ingresar indebidamente a esta dependencia. **Evidencia: SFEV09**	

RECOMENDACIÓN
Proteger la ventana interna y la puerta de acceso principal de la oficina de Centro de Informatica con antepecho de hierro que no deje espacios para realizar ingresos. También se podría utilizar como medida de protección, vidrios de seguridad blindados y la instalación de un sistema electrónico detector de intrusos. Sino se adoptan las medidas anteriores, debe reforzarse el sistema de seguridad de la entrada al edifico, protegiendo esta puerta con antepechos de hierro o vidrios de seguridad blindados. Se recomienda de igual manera, instalar en esta puerta algún sistema electrónico para detección de intrusos y una cámara de video que capte el movimiento a la entrada del edificio, apoyado por el personal de vigilancia asignado al bloque administrativo.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH10 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 10	
El Centro de Informática no esta dotado con un ningún mecanismo electrónico para detección de intrusos. **Evidencia: SFEV10**	
RECOMENDACIÓN	
Se recomienda instalar un sistema de alarma en los puntos mas vulnerables frente a accesos forzosos como puertas y ventanas. El sistema de alarma debe estar apoyado por el personal de vigilancia que atienda o se presente en el menor tiempo posible en el sitio que esta siendo o ya ha sido violada por el delincuente.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :**SFH11 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 11	
El Centro de Informática cuenta con dos chapas, una de perilla y otra de seguridad, sin embargo representan un elemento muy vulnerable a intentos de violación, puesto que fácilmente con un carnét puede abrirse. **Evidencia: SFEV11**	

RECOMENDACIÓN
Instalar por lo menos una chapa de seguridad de cuatro cilindros por tres vueltas, adicional sugerimos la instalación de un sistema electrónico detector de intrusos que respalde el sistema de entrada al Centro de Informática.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH12 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 12	
Se encuentran fisuras en la masilla que asegura y sella los vidrios de las ventanas exteriores, lo que puede permitir la entrada de pequeñas cantidades de agua de lluvia o la filtración de polvo. **Evidencia: SFEV12**	
RECOMENDACIÓN	
Masillar las ventanas de forma compacta, preferiblemente utilizar silicona. Realizar un mantenimiento periódico a las instalaciones físicas del Centro de Informática en que se verifique las condiciones de las ventanas.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH13 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 13

Es notable que la distribución de espacios del Centro de Informática no satisface todas las necesidades de esta dependencia, su diseño se realizo teniendo en cuenta el personal y equipos existentes hasta la fecha del diseño, no se considero el incremento de personal, equipos y el espacio suficiente para almacenar de manera adecuada las grandes cantidades de papelería, equipos y disponer de cintoteca, discoteca y un adecuado cuarto de máquinas.

Evidencia: SFEV13-SFEV04

RECOMENDACIÓN

Redefinir el diseño para optimizar la distribución de espacios del Centro de Informática, de acuerdo a sus necesidades.

Permitir que el personal del Centro de Informática, participe de forma activa en eventuales construcciones o diseño para el Centro de Informática para definir el la distribución de esta dependencia, así como el diseño de la red de datos y red eléctrica.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH14 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 14	
El Centro de Informática no dispone de suficiente espacio para almacenar equipos y papelería, razón por la que se encuentran estos elementos en los pasillos. **Evidencia: SFEV14**	
RECOMENDACIÓN	
Rediseñar la distribución de espacios del Centro de Informática y asignar un mayor espacio para el almacenamiento de papelería. Para futuras construcciones o adecuaciones de espacios, se recomienda que el director del Centro de Informática, participe de forma activa en el diseño para que sea el, quien defina los requerimientos de espacio para la dependencia.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. : SFH15** **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 15	
El Centro de Informática no dispone de un espacio asignado para el mantenimiento de equipos y manipulación e dispositivos. **Evidencia: SFEV15**	
RECOMENDACIÓN	
Establecer un área para el mantenimiento de equipos, la cual debe disponer las herramientas necesarias para este proceso y el almacenamiento de	

dispositivos.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH16 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 16	
El Centro de Informática no dispone de un área adecuada para atención al público, por ésta razón tienen que realizarla a través de una ventana que comunica hacia la parte de afuera del edificio. Este hecho hace que cuando llueve se dañen los documentos entregados a los usuarios. **Evidencia: SFEV16**	

RECOMENDACIÓN
Rediseñar la distribución de espacios en el Centro de Informática y adecuarlos de manera que faciliten el desempeño de sus actividades con una debida atención al público sin que irrumpa cerca del área de programadores. Se recomienda también, que el Centro de Informática no adopte funciones que le corresponden a la dependencia de Tesorería y Pagaduría como es la entrega de liquidaciones.

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DEL CONTROL AMBIENTAL

OBJETIVO

Evaluar que las condiciones ambientales sean las adecuadas para el procesamiento de datos y para la preservación de los equipos.

EVALUACIÓN DEL CONTROL AMBIENTAL EN EL CENTRO DE INFORMÁTICA (C.I)	**REF: SFC06** **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Temperatura				
Se encuentran instalados medidores de temperatura?		X		SFH17
Se mantiene control de temperatura constante?			X	
Las condiciones de temperatura del Centro de Informática son adecuadas para los equipos y el personal?	X			
Existe un sistema de aire acondicionado?		X		SFH18
Humedad				
Se encuentran instalados medidores de humedad?		X		SFH19
Se mantiene control de humedad constante?			X	

Las condiciones de humedad del Centro de Informática son adecuadas para los equipos y el personal?	X			

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. : SFH17** **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 17	
El Centro de Informática no dispone de un termómetro para controlar la temperatura en el cuarto de máquinas y los sitios de trabajo. **Evidencia: SFEV17**	
RECOMENDACIÓN	
Instalar un termómetro que indique de manera constante la medida de la temperatura del cuarto de máquinas y los sitios de trabajo. Este dispositivo debe manejar un sistema de alerta audible que se active cuando la temperatura	

no se registre dentro de los valores normales que corresponde entre 18°C y 24°C.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. : SFH18** **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 18	
El Centro de Informática no dispone de un sensor para controlar la humedad relativa en el cuarto de máquinas y los sitios de trabajo.	

Evidencia: SFEV17
RECOMENDACIÓN
Instalar un que indique de manera constante la medida de la humedad relativa del cuarto de máquinas y los sitios de trabajo. Este dispositivo debe manejar un sistema de alerta audible que se active cuando la humedad relativa no se registre dentro de los valores normales que corresponde entre los 30% y 50%.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. : SFH19** **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 19
El cuarto de maquinas y equipos para proceso de datos del Centro de Informática no posee un sistema de aire acondicionado. **Evidencia: SFEV17**
RECOMENDACIÓN
Proveer de un sistema de aire acondicionado dedicado al cuarto de máquinas y equipos para el proceso de datos de forma exclusiva. La entrada del aire acondicionado debe protegerse con una red metálica para evitar que sea extraído sin autorización y permita acceso a la dependencia.

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DE LA SEGURIDAD FRENTE A DESASTRES

OBJETIVO

Evaluar las medidas preventivas frente algún tipo de desastre, y las acciones de respuesta cuando este se presenta, de manera que eviten daños sustanciales en los equipos, el personal y garanticen la continuidad del sistema.

EVALUACIÓN DE LA SEGURIDAD FRENTE A DESASTRES EN EL CENTRO DE INFORMÁTICA	**REF: SFC07** **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Incendios				
Existe alarma contra incendios?		X		SFH20
La alarma es perfectamente audible?			X	
Existen detectores de humo y de fuego en: Área del centro de cómputo? Perímetro de las instalaciones?		 X X		SFH20
Estos detectores se encuentran distantes de los aparatos de aire acondicionado?			X	

El Centro De Informática dispone de un extintor manual de CO2?		X		SFH21
Acerca de los extintores del Centro de Informática: - Es suficiente el número de extintores? - Es adecuada la capacidad? - Son de fácil acceso? - El peso facilita su uso? - Tienen etiqueta para el control de recarga? - Tienen etiqueta que indiquen la forma de uso? - Su ubicación se encuentra señalizada?			 X X X X X X X	
Existen gabinetes contra incendios en el edificio?	X			

EVALUACIÓN DE LA SEGURIDAD **FRENTE A DESASTRES** **EN EL CENTRO DE INFORMÁTICA**	**REF:** SFC08 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
El vidrio de los gabinetes contra incendio es de seguridad?		X		SFH22
Acerca de los extintores del edificio: - Es suficiente el número de extintores? - Es adecuada la capacidad? - Son de fácil acceso? - El peso facilita su uso? - Tienen etiqueta para el control de recarga? - Tienen etiqueta que indiquen la forma de uso? - Su ubicación se encuentra señalizada?	 X X X X X 	 X X		SFH23
El personal del Centro De Informática se encuentra entrenado en el uso de los extintores?		X		SFH24
La ubicación del Centro De Informática I facilita el ingreso del cuerpo e bomberos?	X			
El cuerpo de bomberos ha sido informado con anterioridad de la vulnerabilidad de los equipos que aquí se ubican?		X		SFH25

Existe un hidrante cerca del edificio donde se encuentra el Centro De Informática?	X			
Se encuentran señaladas las salidas?		X		SFH26
Se encuentra capacitado el personal del Centro De Informática en procedimientos frente a incendios?		X		SFH24
Esta prohibido fumar del área de cómputo?	X			
El inmobiliario del Centro De Informática es incombustible?		X		SFH27
Inundaciones				
Las cañerías cercanas al Centro De Informática se encuentran en buen estado?	X			
Existen canales de drenaje en el entorno del Centro De Informática?	X			
Los desagües se encuentran limpios?	X			
EVALUACIÓN DE LA SEGURIDAD **FRENTE A DESASTRES** **EN EL CENTRO DE INFORMÁTICA**	**REF:** SFC09 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
El techo del Centro De Informática es impermeable?	X			
El centro de informática esta exento de aspersores contra incendio en base a agua?	X			
Se cuenta con bombas de emergencia para resolver inundaciones?		X		SFH28
Los hidrantes se encuentran distantes del Centro de Informatica?		X		SFH29
Se evita la ubicación de equipos de cómputo a nivel del suelo?		X		SFH30
Terremoto				
La construcción se ha realizado bajo las normas de sismo resistencia?	X			

Los equipos se encuentran ubicados en áreas no elevadas?	X			
Existen procedimientos para evacuación?	X			
Existen pólizas de seguros que cubran el riesgo y la cuantía en casos de siniestros?	X			
Sabotaje				
En caso de tomas al bloque administrativo, se cierran los sistemas?	X			
Se cierra con llave la oficina?	X			
Emergencias				
Existe una cartelera en el Centro De Informática que informe los teléfonos de: - Policía - C.A.I. - Bomberos - E.P.S y A.R.S		X		SFH31

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH20 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 20	
El Centro de informática y el perímetro de las instalaciones no están provistos de dispositivos para detección de humo o fuego. **Evidencia:** SFEV18	
RECOMENDACIÓN	
Instalar en el cuarto de máquinas del Centro de informática, en el área de trabajo de los funcionarios y en pasillos del bloque administrativo detectores de humo y fuego, con alarma, que alerten de la presencia de fuego.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH21 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 21	
El Centro de informática dentro de su dotación, no dispone de un extintor de incendios. **Evidencia:** SFEV19	
RECOMENDACIÓN	
Dotar al Centro de Informática con un extintor tipo C, con capacidad de 5 Kg., el cual debe recibir el mantenimiento periódico correspondiente.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH22 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 22	
En el primer piso del edificio, donde se ubica el Centro de Informática se encuentra un gabinete contra incendios, este se encuentra cerrado con llave de la cual el personal del centro de informática y las dependencias de este edificio no tienen conocimiento. El vidrio con el cual esta protegido este gabinete no es	

de seguridad, este hecho afecta en la medida que cuando se presente una emergencia debe romperse el vidrio del gabinete corriendo el riesgo de sufrir accidentes. **Evidencia:** SFEV20
RECOMENDACIÓN
Colocar al gabinete contra incendios vidrio de seguridad y disponer al lado de un martillo para poder romperlo. Tener una copia de la llave del gabinete donde se encuentra el extintor y demás elementos y herramientas contra incendios. Dotar al bloque administrativo de más extintores, distribuidos adecuadamente.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH23 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 23	
En el edificio donde se localiza el Centro de Informática no cuenta con el adecuado numero de extintores según el numero de oficinas. **Evidencia:** SFEV20	
RECOMENDACIÓN	
Dotar a cada una de las oficinas del Bloque Administrativo de un extintor tipo C y en el espacio libre del edificio localizar extintores tipo C uno cada 15m o distribuidos adecuadamente en cada piso y realizar el mantenimiento periódico de dichos extintores.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH24 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 24	
El personal del Centro de Informática no se encuentra capacitado en el manejo de extintores y en los procedimientos a realizar frente a un incendio. **Evidencia:** SFEV21	
RECOMENDACIÓN	
Se debe capacitar al personal que trabaja en las instalaciones en el manejo de dispositivos contra incendio y procedimientos de evacuación frente a posibles incendios o cualquier otro tipo de desastre, considerando que estamos en una zona de actividad volcánica. Se recomienda establecer en la Universidad de Nariño un plan de prevención de desastres y evacuación el cual sea comunicado al personal de la Universidad.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH25 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 25	
El cuerpo de bomberos no ha sido informado de la ubicación y vulnerabilidades de los equipos que se encuentran en el centro de informática. **Evidencia:** SFEV22	
RECOMENDACIÓN	
Informar con anterioridad al cuerpo de bomberos de la ubicación y	

vulnerabilidad de los equipos, de manera que al presentarse una emergencia ellos realicen el procedimiento adecuado para no irrumpir en daños mayores.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH26 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 26	
La salida del Centro de Informática y del Bloque Administrativo no se encuentra señaladas para realizar una evacuación adecuada en caso de presentarse un incendio y el humo dificulte la visibilidad del sitio.	

Evidencia: SFEV23
RECOMENDACIÓN
Señalizar las salidas del Centro de Informática, dependencias y Bloque administrativo para realizar una evacuación adecuada en caso de presentarse un incendio. Se recomienda realizar esta señalización también a nivel del piso puesto que el humo impide mirar hacia una parte superior.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH27 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 27	
Las divisiones internas del Centro de Informática, al igual que muebles, papeleras y puertas son de material combustible, estos elementos facilitan la propagación del fuego en caso de presentarse un incendio. **Evidencia:** SFEV07	
RECOMENDACIÓN	
Evitar dentro del Centro de Informática elementos de fácil combustión y remplazarlos por objetos de material incombustible.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH28 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 28	
No se dispone de una bomba para extracción de agua de emergencia para resolver problemas de inundaciones. **Evidencia:** SFEV24	
RECOMENDACIÓN	
Se recomienda mantener una bomba en el Bloque Administrativo exclusiva para atender emergencias de inundaciones. Se debe establecer que el personal de mantenimiento le realice pruebas, para garantizar su funcionamiento.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH29 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 29	
Los hidrantes son una medida de aseguramiento en caso de incendios, sin embargo el hidrante que respalda al Bloque Administrativo, se localiza frente del Centro de Informática, al presentarse algún daño en el hidrante el Centro de Informática queda expuesto a una presión fuerte de agua, la cual puede provocar una inundación causando daños en los equipos y pérdida de información. **Evidencia:** SFEV25	

RECOMENDACIÓN
El hidrante, no debe localizarse cerca del Centro de Informática.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH30 **Fecha :** Marzo / 2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 30	
En caso de inundación se corre el riesgo de la pérdida de equipos y de papelería que se ubican a nivel del suelo.	

Evidencia: SFEV26
RECOMENDACIÓN
Establecer un sitio adecuado para el almacenamiento de papelería de manera que no tenga que ubicarse en el suelo. Ubicar los equipos en mesas o soportes fuertes, para elevarlos del nivel del suelo.

DE NARIÑO	
HALLAZGO 31	
EL Centro de Informática no tiene a la vista, una lista de los teléfonos de emergencia que agilicen procesos para una rápida atención. **Evidencia:** SFEV27	
RECOMENDACIÓN	
Mantener en una parte visible, una lista de los teléfonos de emergencia como: Policía, C.A.I., Bomberos, E.P.S Y A.R.S, Defensa Civil, Hospital Departamental, nombres de los miembros del comité de emergencia de la Universidad de Nariño.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN DE LOS EQUIPOS

OBJETIVO

Evaluar los procedimientos, de manera que sean los adecuados para proteger a los equipos, mantenerlos libre de fallas y evitar su deterioro.

EVALUACIÓN DE LA SEGURIDAD EN EQUIPOS EN EL CENTRO DE INFORMÁTICA	**REF:** SFC10 **Elaboró:** M.C.T y E.A.F **Fecha :** Abril / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**

Dotación				
Se cuenta con los equipos suficientes para el procesamiento de la información?		X		SFH32
Se tiene computador de respaldo en caso de siniestros		X		SFH32
Se cuenta con UPS?	X			
Se cuenta con planta eléctrica de respaldo?		X		SFH33
Registro				
Se tiene identificado las características de hardware y sus capacidades?	X			
Se lleva un inventario actualizado de equipos?	X			
Los equipos tienen etiqueta de identificación?	X			
Mantenimiento				
Se realiza mantenimiento periódico de los equipos?		X		SFH34
Se lleva un registro escrito de los mantenimientos realizados?		X		SFH34
Es oportuna la atención ante fallos de los equipos?	X			
Se mantienen los equipos tapados?		X		SFH35

EVALUACIÓN DE LA SEGURIDAD EN EQUIPOS EN EL CENTRO DE INFORMÁTICA	**REF:** SFC11 **Elaboró:** M.C.T y E.A.F **Fecha :** Abril / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Asignación				
Se asigna un responsable para el manejo de los equipos?	X			
El uso de los equipos es exclusivo de los funcionaros del Centro de Informática?	X			
La utilización de los equipos es exclusiva para actividades del Centro de Informática?	X			
Movilización				
Existe control de la circulación de equipos dentro del Centro de Informática?	X			
La movilización de equipos en el Centro de Informática es autorizada por el director?	X			
Existe control del ingreso y salida de equipos, a la entrada del bloque administrativo?		X		SFH36
La movilización de equipos es autorizada por el director?	X			
Limpieza				
Esta el Centro de Informática exento de elementos que produzcan polvo?	X			
Recibe el Centro de Informática limpieza constante?	X			
La limpieza es adecuada que le permita mantenerse libre de polvo?		X		SFH37

Se prohíbe el consumo de bebidas y comestibles en el área de cómputo?		X		SFH38

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH32 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 32

Los servidores con que cuenta el Centro de Informática, no son suficientes para realizar el procesamiento de datos, considerando que hace falta un servidor de respaldo para levantar el sistema en casos de siniestros.

Evidencia: SFEV28

RECOMENDACIÓN

Atender la solicitud del Director del Centro de Informática y proveer a la dependencia del Centro de Informática con más servidores que permitan cubrir óptimamente las necesidades del proceso de información de la Universidad y dar mejores servicios.

Tener siempre un servidor de respaldo que se active automáticamente dando respaldo al sistema en caso de que el servidor principal falle.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH33 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 33	
El Centro de Informática no cuenta con planta eléctrica de respaldo. **Evidencia:** SFEV29	

RECOMENDACIÓN
Dotar al Centro de Informática con una planta eléctrica de combustible, que permita la continuidad del trabajo cuando se presente interrupción del suministro eléctrico normal y permita continuar trabajando con los procesos críticos o urgentes.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH34 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 34

Los equipos del Centro de Informática no reciben mantenimiento periódico, el mantenimiento se realiza cuando se presentan fallos, sin establecer por escrito las falencias encontradas.

Evidencia: SFEV30

RECOMENDACIÓN

Realizar mantenimiento a los equipos una vez por año y llevar una planilla de mantenimientos preventivos y correctivos, con el listado de los equipos, características, fecha del mantenimiento, fallas detectadas y nombre del responsable.

El mantenimiento lo debe realizar personal especializado que acredite experiencia en dichas labores.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH35 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 35	
Los equipos del Centro de Informática se encuentran equipos destapados, lo cual puede provocar daños o pérdida de las partes del equipo. **Evidencia:** SFEV31	
RECOMENDACIÓN	
Los equipos deben estar completamente tapados, tanto el chasis como las bahías de los dispositivos.	

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFEV36 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 36

En el bloque administrativo, no existe control de la entrada y salida de equipos de computo.

Evidencia: SFH32

RECOMENDACIÓN

Delegar a la persona que se encuentra a la entrada del Bloque Administrativo, realizando el control de acceso de personas, que controle la movilización de equipos en el bloque, registrando en una planilla: tipo de equipo, marca, número de serie, características, nombre y número de identificación de la persona que lo porta, al igual que el nombre de la persona que autoriza. La autorización para la entrada o salida de equipos, debe realizarse por escrito, firmada por el jefe de la dependencia involucrada.

Si los equipos, van a ser traslados permanentemente de oficina, debe informarse a la oficina de Almacén y Compras, del cambio efectuado.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH37 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 37

La limpieza al Centro de Informática se realiza de manera constante, sin embargo no es de manera adecuada puesto que la disposición de cableado, equipos y otros elementos dificultan la realización de éste trabajo, ocasionando acumulaciones de polvo y basura que pueden afectar el funcionamiento de las máquinas.

Evidencia: SFEV33

RECOMENDACIÓN

Organizar el tendido de cableado, equipos y otros elementos que se encuentran en lugares que obstaculizan los procesos de aseo.

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SFH38 **Fecha :** Abril/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 38	
No existe una política que prohíba el consumo de comestibles o bebidas dentro del área de trabajo o cerca de los equipos de computo, poniendo en riesgo los computadores frente a posibles accidentes. **Evidencia:** SFEV34	

RECOMENDACIÓN
Establecer una norma que prohíba el consumo de bebidas y comestibles en el área de trabajo y cerca de los equipos de cómputo.

SFEV01

EXTERIOR CENTRO DE INFORMATICA.

EXTERIOR BLOQUE ADMINISTRATIVO

EXTERIOR CENTRO DE INFORMATICA, DENTRO DEL BLOQUE ADMINISTRATIVO

SFEV02

plano

SFEV03

Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX04)

1. ¿Cuándo fue la construcción del bloque administrativo, donde se localiza el Centro de Informática, fueron consideradas opiniones o sugerencias de parte suya?¿Cuáles?
Sí, se hicieron sugerencias sobre todo en ductería que se debería utilizar para el cableado del Centro de Informática y del edificio, pero no fueron atendidas.
2. ¿Participó Usted en el diseño y asignación de espacios dentro del Centro de Informática?
No
8. ¿Se tiene un área exclusiva para reuniones de oficina?
El área de reuniones es simplemente el área que hay en la oficina de la dirección del Centro de Informática.
10 ¿Se provee de un lugar para la bóveda de seguridad, altamente protegido?
No existe dentro de la universidad ni en particular en el Centro de Informática lugar para una bóveda de seguridad.
11. ¿Existe un lugar asignado para el almacenamiento de equipos fuera de uso?
Los equipos que quedan fuera de uso simplemente se dan de baja y no hay un lugar designado para este almacenamiento.

SFEV04

CINTAS DE RESPALDO.
CUBÍCULO DE TRABAJO

CUBÍCULOS DE TRABAJO.
CENTRO DE INFORMÁTICA

EQUIPOS FUERA DE USO.
ENTRADA DEL CENTRO DE INFORMÁTICA

PAPELERÍA EN CAJAS DE CARTÓN.
CUARTO DE MAQUINAS

SFEV05
Auto Narración

Se solicitó, a la Oficina de Planeación de la Universidad de Nariño, mediante oficio con fecha del 27 Enero de 2004 (Anexo ANX01), planos de instalaciones, planos red eléctrica, planos red de datos, planta de personal, manual de funciones y procedimientos del Centro de Informática.

De la anterior solicitud se obtuvo de la Oficina de Planeación, mediante acta de entrega con fecha Febrero 3 de 2004 (Anexo ANX02), los planos de instalaciones, correspondientes al primer piso del bloque administrativo donde se localiza el Centro de Informática, el cual no corresponde a la distribución actual del primer piso del bloque administrativo. Los demás planos solicitados no se entregaron debido a que no existen en la Oficina de Planeación.

De igual manera la Oficina de Planeación hizo entrega del manual de funciones y procedimientos del Centro de Informática.

SFEV06

Auto Narración

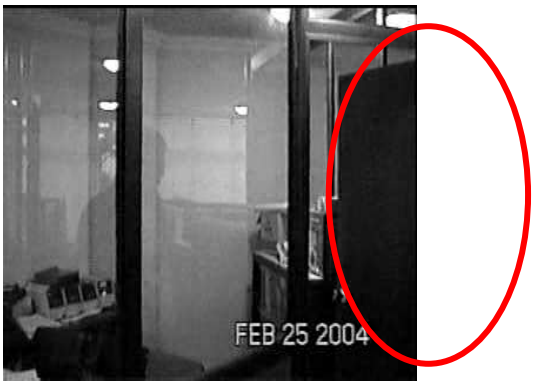
Se realizo la solicitud de los planos de la red de datos (ANX01) al Centro de Informática y a la oficina de Planeación, sin embargo debido a la ausencia de los mismo estos no fueron entregados. Se dijo que el arquitecto los tenia, se hizo contacto con el arquitecto responsable de la obra, se comprometió a entregarlos, pero no lo hizo.

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

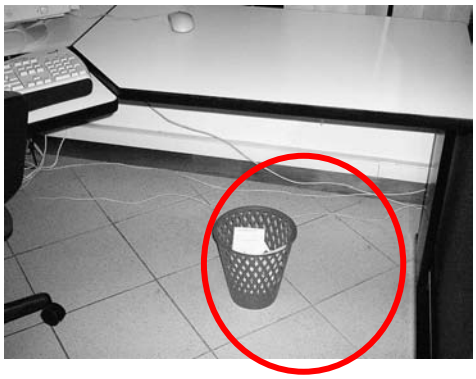
1. ¿Existe el Diseño de la red de datos?
La empresa que fue contratada para hacer el diseño de la red dejo únicamente, el cableado que hay entre el tablero y los puntos, los puntos no fueron numerados correctamente, razón por la cual debido a que de todas formas tocaba hacer la instalación de los computadores nosotros reasignamos el numero de los puntos, en el momento entonces las cajas de las oficinas tienen su numero correspondiente con el panel central.

SFEV07

PUERTA BODEGA



PUERTA OFICINA DIRECTOR



PAPELERA PLÁSTICA EN PUESTO DE TRABAJO

PAPELERA DE CARTÓN OFICINA DIRECTOR

DIVISIONES EN MADERA

SFEV08

DIVISIONES INTERNAS EN PAÑO

SFEV09

PUERTA DE ACCESO A CENTRO DE INFORMÁTICA

VENTANA EXTERIOR DEL CENTRO DE INFORMÁTICA DENTRO DEL BLOQUE ADMINISTRATIVO

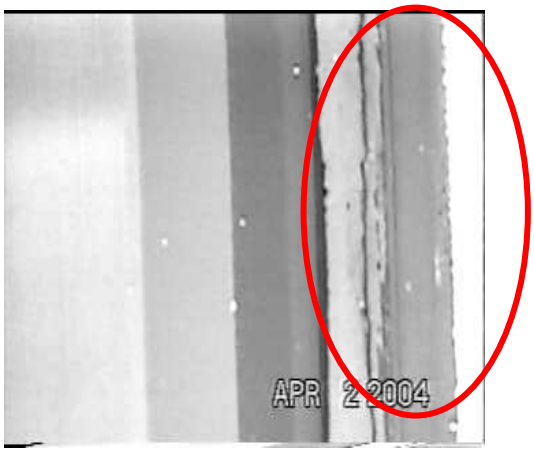
SFEV10

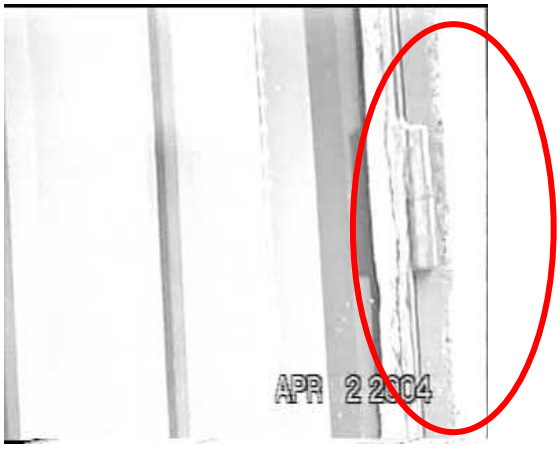
PUERTA DE ACCESO PRINCIPAL
CENTRO DE INFORMÁTICA

SFEV11

CHAPAS PUERTA ACCESO PRINCIPAL
CENTRO DE INFORMÁTICA

SFEV12





VENTANA CENTRO DE INFORMÁTICA
EXTERIOR BLOQUE ADMINISTRATIVO

SFEV13
Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX04)

4. ¿Considera que el espacio que se dispone es suficiente para albergar todos los equipos de informática?
No, el espacio no es el suficiente para todas las necesidades del Centro de Informática.

SFEV14

ENTRADA CENTRO DE INFORMÁTICA

PASILLO ENTRADA CUARTO DE MAQUINAS

SFEV15
Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX04)

6. ¿Se encuentra establecida un área para el mantenimiento de equipos?
No hay un área para el mantenimiento de equipos de hecho no se necesita pero no hay el espacio disponible.

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

18. ¿Cuentan con un sitio adecuado para el mantenimiento y con las herramientas adecuadas para realizar esta actividad?
No, algunas herramientas como el ventilador cuando se quita el polvo, no lo presta otra oficina, la oficina de Contabilidad y equipo para el resto solo se necesita un destornillador de estrella para ajustar o aflojar algunas tarjetas de control, tenemos la ponchadota, no tenemos un probador para los puntos de red, eso no lo suministra el Aula de Informática.

SFEV16

EXTERIOR CENTRO DE INFORMÁTICA

EXTERIOR CENTRO INFORMÁTICA DENTRO DEL BLOQUE ADMINISTRATIVO

SFEV17
Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX04)

12. ¿Se mantiene algún control de temperatura y de humedad?¿Se realiza de manera constante?

No se hace control de temperatura y humedad tanto en el Centro de Informática como en el área donde se presta los servicios de comunicaciones e Internet, de hecho se hizo la solicitud de una unidad de aire acondicionado para el área donde están los servidores, pero esta petición no ha sido atendida hasta el momento..

SFEV18

CUARTO DE MAQUINAS

ÁREA DE TRABAJO DE FUNCIONARIOS

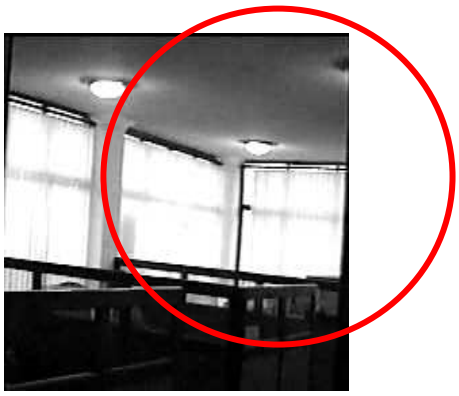
PERÍMETRO CENTRO INFORMÁTICA
INTERIOR BLOQUE ADMINISTRATIVO

SFEV19

Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX03)

Digamos aquí no tenemos una seguridad física … bueno no solo nosotros sino todo el edificio busque un extintor y no encuentra uno

VISTA GENERAL FRENTE
CENTRO DE INFORMÁTICA



VISTA GENERAL COSTADO IZQUIERDO
CENTRO DE INFORMÁTICA

CUARTO DE MAQUINAS
CENTRO DE INFORMÁTICA

OBSERVACIÓN: NO EXISTE UN EXTINTOR DE INCENDIOS

SFEV20

EXTINTOR – CHAPA CON LLAVE

ÚNICO GABINETE CON HERRAMIENTAS CONTRA INCENDIOS EN EL BLOQUE ADMINISTRATIVO, ASEGURADO CON LLAVE

SFEV21

Entrevista Realizada Programador Centro De Informática
Cuestionario No. 1 (Anexo ANX05)

¿Conoce los procedimientos a seguir frente a posibles desastres? (incendios, inundaciones, terremotos, disturbios)
Salir corriendo, los equipos ahí cualquier cosa se hace de algunas cosa tengo copia en mi casa.

¿Ha participado de simulacros que indiquen los pasos y el modo de evacuación ante percances como los mencionados anteriormente?
Nada, una vez me hicieron un examen de la visión de riesgos profesionales.

¿Conoce como funciona un extintor?
Pues yo tengo uno en mi carro creo que ha de funcionar lo mismo.

SFEV22

Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX03)

14. ¿El departamento de bomberos ha sido informado previamente de las características y vulnerabilidades del C.I.?
No, de hecho ninguna dependencia en la Universidad ha hecho este tipo de peticiones.

SFEV23

SALIDA BLOQUE ADMINISTRATIVO

INTERIOR BLOQUE ADMINISTRATIVO

SALIDA CENTRO DE INFORMÁTICA

SFEV24

Entrevista Funcionario de Servicios Generales, Brayan Betancourth

¿La Universidad cuenta con bombas de emergencia para casos de inundación?
No, de eso no tiene nadie, ni aquí ni en ninguna dependencia.

SFEV25

EXTERIOR BLOQUE ADMINISTRATIVO

SFEV26

PUESTO DE TRABAJO

CUARTO DE MAQUINAS

CUARTO DE MAQUINAS

SFEV27

Auto Narración

Revisando las instalaciones del Centro de Informática, se pudo observar que no existe una cartelera informativa que haga referencia a los teléfonos de emergencia.

SFEV28
Entrevista Realizada Director Centro de Informática
Cuestionario No. 2 (Anexo ANX03)

¿Se cuenta con los equipos suficientes?
No se cuenta con los equipos suficientes, de hecho se necesitan unos tres servidores adicionales a los que ya existen.

SFEV29

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 3 (Anexo ANX07)

¿Tiene un sistema de respaldo en el sentido de Planta Eléctrica?
No, no hay planta eléctrica de respaldo. ¿La Planta que tienen la Universidad en la parte de abajo? –Esta dañada, esta de adorno, creo que era solo para el Centro Administrativo que antes funcionaba allá, en el tiempo que yo estoy no la he visto funcionar .

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

21. ¿Cuentan con planta de respaldo eléctrico?
No, simplemente la oficina, tiene una UPS con capacidad de 2000.

Entrevista Funcionario Servicios Generales Brayan Betancourth

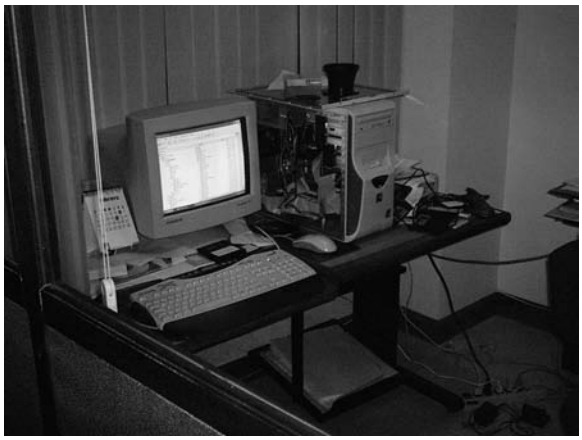
¿El bloque administrativo cuenta con planta eléctrica de respaldo?
No, aquí ósea planta eléctrica que se maneje no.

SFEV30

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

En lo que se refiere a mantenimiento de equipos, ¿Cada cuanto se realiza mantenimiento?
Aproximadamente cada dos meses, entonces hacemos mantenimiento preventivo básicamente en quitar un poquito de estática a los computadores, quitarles un poco de polvo, pero realmente como los sistemas permanecen prendidos toda la semana, es difícil apagar el sistema y realizar su mantenimiento, y prácticamente los mantenimientos son de...los discos duros son Scsi son de buena calidad realmente son discos duros que están elaborados para trabajar todos los días del año, sin ningún problema, muchas veces el mantenimiento resulta contraproducente porque en lugar de hacerle un beneficio al equipo, puede dañarle la información, mas bien evitamos un poco tocar los servidores.

SFEV31



OFICINA DIRECTOR
CENTRO DE INFORMÁTICA

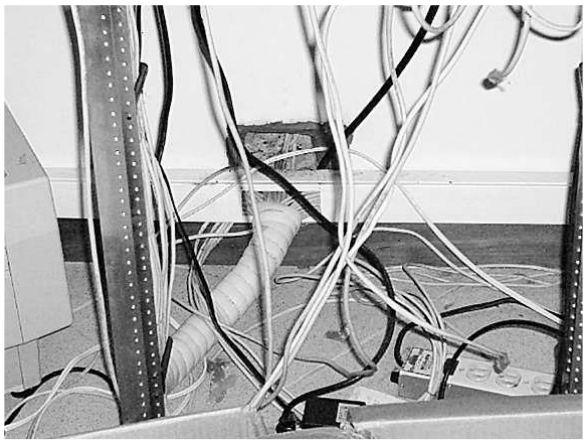
CUARTO DE MAQUINAS
CENTRO DE INFORMATICA

SFEV32

VISTA EXTERIOR
BLOQUE ADMINISTRATIVO

NO EXISTE UN CONTROL DE ACCESO A LA ENTRADA DEL BLOQUE ADMINISTRATIVO

SFEV33



CENTRO DE CABLEADO
CUARTO DE MAQUINAS

CUARTO DE MAQUINAS

CUARTO DE MAQUINAS

SFEV34

Entrevista Realizada al Director del Centro de Informática
Cuestionario No. 2 (Anexo ANX04)

21. ¿Se prohíbe el consumo de bebidas y comestibles en el área de cómputo?
No

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD FÍSICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

EVALUACIÓN REDES ELECTRICAS

OBJETIVO

-Determinar el estado de la red eléctrica del Centro de Informática revisando si el cableado, puesta a tierra balance de cargas son adecuados.
-Verificar que los elementos de la red eléctrica se adhieran a estándares establecidos

EVALUACIÓN DE LA RED ELECTRICA DEL CENTRO DE INFORMÁTICA	**REF:** SEC01 **Elaboró:** M.C.T y E.A.F **Fecha:** Mayo / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Existe una conexión de puesta a tierra con capacidad para soportar la carga conectada?	X			
Cuenta con pararrayo?		X		SEH01
Se realizan mantenimientos periódicos preventivos de los equipos eléctricos y redes eléctricas?		X		SEH02
Se inspecciona periódicamente el estado de las redes e instalaciones locativas eléctricas, equipos?		X		SEH02

Se maneja la siguiente codificación de colores en las instalaciones eléctricas: Neutro : blanco Fase : negro Tierra de protección: verde o desnudo Tierra de asilada: verde/amarillo?	X			
Los equipos se encuentran conectados a reguladores de corriente eléctrica?		X		SEH03
Los reguladores de corriente mantienen la carga adecuada?		X		SEH04
Los equipos se conectan correctamente a la corriente eléctrica?		X		SEH05

EVALUACIÓN DE LA RED ELÉCTRICA DEL CENTRO DE INFORMÁTICA	**REF:** SEC02 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Las instalaciones eléctricas cuentan con señalización que determine que tipo de corriente maneja?		X		SEH06
Las instalaciones eléctricas se encuentran correctamente instaladas.?		X		SEH07
El transformador utilizado, posee la potencia suficiente para soportar la carga conectada al circuito?	X			
El transformador utilizado esta provisto con placa que especifique sus características?	X			
La tubería tiene resistencia al fuego de por lo menos 15 min?	X			
El cableado eléctrico esta debidamente conectado, neutro, fase y tierra?	X			
Los cables se encuentran correctamente instalados a los toma corrientes?	X			
La puesta a tierra se ubica en un lugar húmedo?	X			

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH01 **Fecha :** Junio /2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 01	
El Centro de Informática no cuenta con un pararrayo. **Evidencia** :SEEV01	
RECOMENDACIÓN	
Instalar de un pararrayo que respalde el circuito eléctrico incluyendo la puesta a tierra, se recomienda además que se realice la revisión del documento de Normas Técnicas Eléctricas Colombianas RETIE (ANEXO 12), en donde se plantea una correcta instalación del pararrayo.	

EVALUACIÓN A LA SEGURIDAD RED ELÉCTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH02 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 02	
No se realizan inspecciones, ni mantenimientos periódicos preventivos de los equipos, instalaciones locativas de las dependencias, redes eléctricas y alumbrado. **Evidencia :** SEEV02	
RECOMENDACIÓN	
Las acciones preventivas, permiten minimizar las acciones correctivas, de tal forma que los problemas se los pueden reducir a través de estas acciones, debe ser compromiso de las personas encargadas del mantenimiento de las instalaciones realizar periódicamente mantenimientos preventivos.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH03 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 03	
Algunos de los equipos instalados en las oficinas no se encuentran conectados a reguladores de corriente eléctrica. **Evidencia** :SEEV03	
RECOMENDACIÓN	
Conectar los equipos a reguladores de corriente, con especificaciones según la carga eléctrica que deban soportar.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH04 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 04	
Se aprecia que existen reguladores eléctricos, multitomas, y toma corrientes que se encuentran sobre cargados de equipos conectados. **Evidencia** : SEEV04	
RECOMENDACIÓN	
Establecer circuitos eléctricos específicos para la conexión de equipos de oficina y circuitos regulados para equipos de cómputo.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH05 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 05	
Se presentan problemas en las conexiones e instalaciones de los equipos a los estabilizadores, multitomas y tomacorrientes. **Evidencia** : SEEV05	
RECOMENDACIÓN	
Capacitar a los usuarios en el manejo y correcta conexión de los equipos a los toma corrientes.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH06 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 06	
Las redes eléctricas no se encuentran señalizadas, por lo cual no se puede determinar si es corriente regulada o no regulada, con conexión a UPS, o sin respaldo. **Evidencia** :SEEV06	
RECOMENDACIÓN	
Etiquetar los toma corriente de tal manera que los funcionarios identifiquen que tipo de corriente corresponde y puedan realizar las conexiones de manera adecuada.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH07 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 07	
Se presentan sectores en donde se evidencia que la tubería no metálica no se encuentra correctamente instalada, tomas y cables sueltos. **Evidencia** : SEEV07	
RECOMENDACIÓN	
Realizar ajusten en las instalaciones eléctricas solucionando los problemas actuales, se debe garantizar por el personal encargado, una instalación correcta de los toma corrientes, evitando la utilización de tomas sobrepuestos, cascadas de multitomas con reguladores, adiciones de cables realizadas por usuarios no especializados.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD DE LA RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

Verificar que se realicen acciones de mantenimiento a la red eléctrica para garantizar el buen estado y funcionamiento de las misma.

EVALUACIÓN DEL MANTENIMIENTO DE LA RED ELECRTICA	**REF:** SEC03 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se realiza mantenimiento preventivo periódico a las conexiones de la red eléctrica?		X		SEH08
El mantenimiento preventivo se realiza revisando: • Estado de limpieza • Si hay presencia de oxido • Si hay humedad • Si hay quemaduras • Ennegrecimiento • Roturas • Tornillos flojos • Cables sueltos • Tomacorrientes dañados • Lámparas quemadas			X	

Se registran los resultados de la inspección, las fallas importantes y las acciones que se ejecutan en el mantenimiento?		X		SEH09
Las acciones de corrección se planifican de acuerdo a la importancia y urgencia de las misma?	X			
Se atienden oportunamente las correcciones ante fallas?	X			
Se realiza mantenimiento preventivo a la conexión de puesta a tierra.		X		SEH10

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH08 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.

HALLAZGO 08

Las conexiones eléctricas no reciben mantenimiento preventivo, en el cual se realice limpieza y verificación de su estado para determinar posibles fallas que puedan ocurrir.

Evidencia : SEEV08

RECOMENDACIÓN

Realizar periódicamente una revisión de las conexiones eléctricas de la universidad, en la que se realice mantenimiento preventivo, teniendo en cuenta por lo menos la limpieza, si existe presencia de humedad, presencia de oxido, rupturas, cables sueltos toma corrientes dañados y realizar la correspondientes reparaciones.

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH09 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 09	
Las reparaciones realizadas a los daños eléctricos no se registran en documentos escritos que especifique, ubicación, tipos de daños y acciones realizadas. **Evidencia** : SEEV09	
RECOMENDACIÓN	
Registrar en un documento escrito, en el que se especifiquen dependencia donde ocurre el daño, diagnostico, acciones realizadas, hora en que ocurrió el daño, hará de solución, responsable.	

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH10 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 10	
Las conexiones de puesta a tierra no reciben mantenimiento preventivo, en el cual se verifique de su estado para garantizar óptimo funcionamiento y evitar posibles fallas de sobre tensiones en lo componentes electrónicos. Evidencia : SEEV10	
RECOMENDACIÓN	
Realizar periódicamente una revisión de las puesta a tierra, en el cual se revise si el nivel de humedad es el adecuado, y el voltaje con el que cuenta esta dentro del que corresponde.	

FORMATO DE CONTROL INTERNO

EVALUACIÓN A LA SEGURIDAD DE LA RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

OBJETIVO

-Revisar que el Centro de Informática, cuente con sistemas de respaldo frente a interrupciones de energía de tal manera que no se vea afectada la continuidad del trabajo.
-Verificar la disponibilidad y buen funcionamiento de los equipos de respaldo

EVALUACIÓN DEL SISTEMA DE ENERGÍA ININTERRUMPIDO DEL CENTRO DE INFORMÁTICA	**REF:** SEC04 **Elaboró:** M.C.T y E.A.F **Fecha:** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
El centro de informática cuenta con planta eléctrica de respaldo?		X		SEH11
La planta eléctrica proporciona energía por varias horas?			X	
El centro de informática cuenta con UPS de respaldo?	X			
La autonomía de las UPS es suficiente para guardar archivos y cerrar el sistema correctamente?	X			
La autonomía de la UPS es suficiente para dar paso a la activación de la planta eléctrica?			X	
Las plantas eléctricas son de uso exclusivo el centro de informática cuando se produce interrupción del abastecimiento normal de energía?			X	
La planta eléctrica se ubica en un sitio distante al centro de informática?			X	
El sitio donde se encuentra la planta eléctrica garantiza la protección de la misma?			X	

El sitio donde se ubica la planta eléctrica, cuenta con ventilación?			X	
Se realiza mantenimiento de la planta verificando: • Nivel de agua en el radiador • Nivel de aceite en el carter • Nivel de agua en celdas de bateria • Nivel de combustible en tanque diario • Limpieza			X	
EVALUACIÓN DEL SISTEMA DE ENERGÍA ININTERRUMPIDO DEL CENTRO DE INFORMÁTICA	**REF:** SEC05 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se prueba periódicamente si la planta esta en optimo funcionamiento?			X	
Las UPS tienen la capacidad adecuada?	X			
Las UPS son revisadas y probadas periódicamente de acuerdo con las especificaciones del fabricante?	X			

EVALUACIÓN A LA SEGURIDAD RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SEH11 **Fecha :** Junio/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 11	
El Centro de Informática no cuenta con un sistema de planta eléctrica de respaldo, que le permita dar continuidad a los procesos que realiza, en caso de presentarse interrupción en el suministro eléctrico por tiempo prolongado. **Evidencia** : SEEV11	
RECOMENDACIÓN	
Dotar al Centro de Informática y las dependencias que mantienen servidores de trabajo con una planta eléctrica de alimentación de combustible y activación automática, con capacidad para mantener los equipos de trabajo funcionando .	

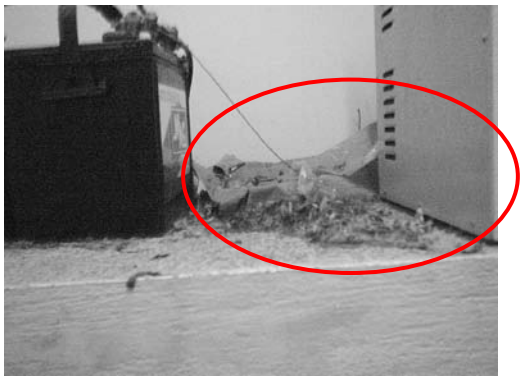
SEEV01

Auto Narración

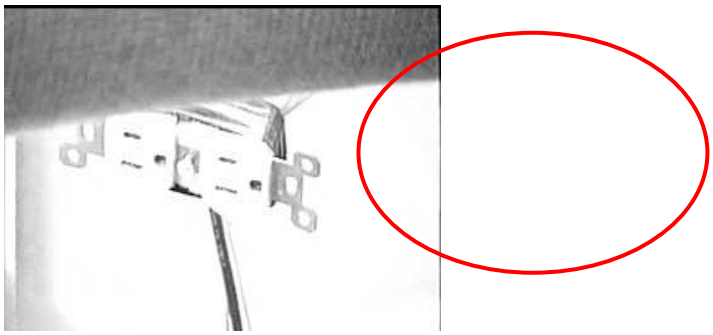
Revisando las instalaciones del bloque administrativo en la parte externa, se observó que no se encuentra una conexión de pararrayo que respalde la instalación eléctrica del centro de informática y demás dependencias ubicadas en este bloque

SEEV02

CENTRO DE INFORMÁTICA

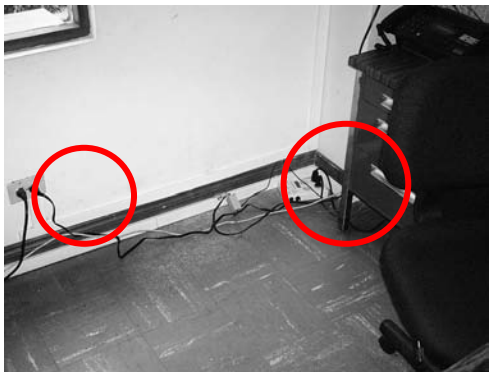


OFICINA OCARA

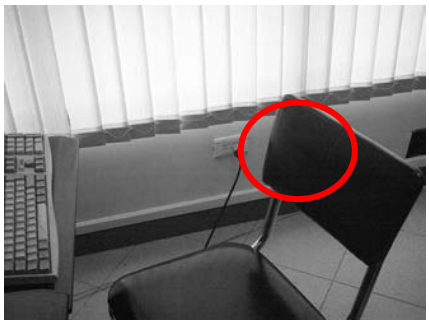


OFICINA CONTABILIDAD

SEEV03

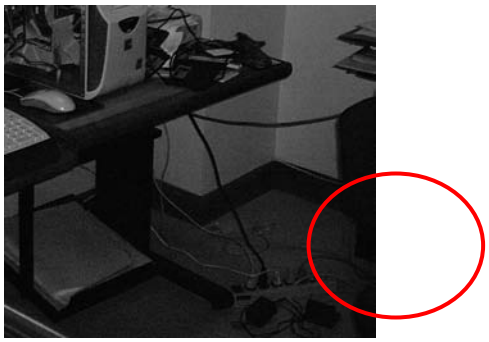


OFICINA ALMACÉN Y COMPRAS



OFICINA TESORERÍA Y PAGADURÍA

SEEV04

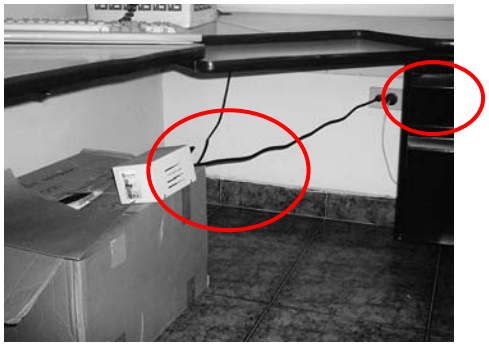


CENTRO DE INFORMÁTICA

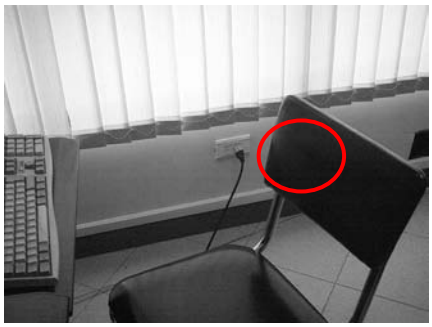
OFICINA TESORERÍA Y PAGADURÍA

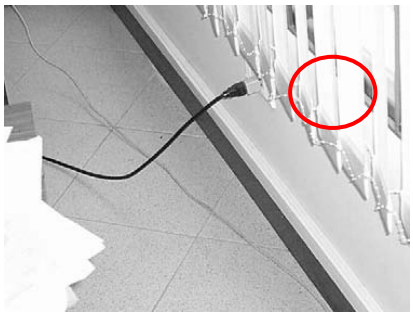
CENTRO DE INFORMÁTICA

SEEV05



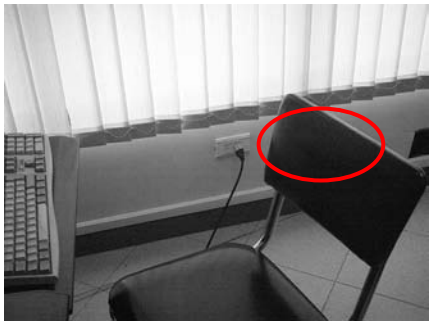
OFICINA OCARA



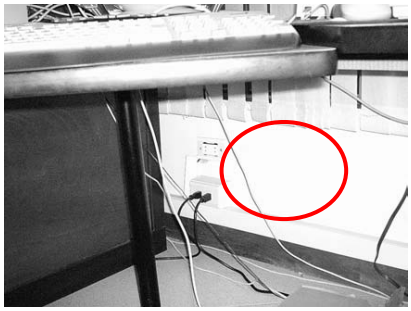


OFICINA TESORERÍA

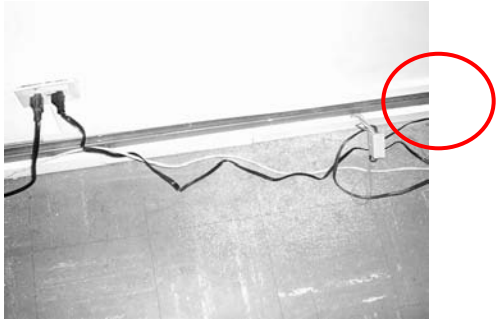
SEEV06



OFICINA TESORERÍA Y PAGADURÍA



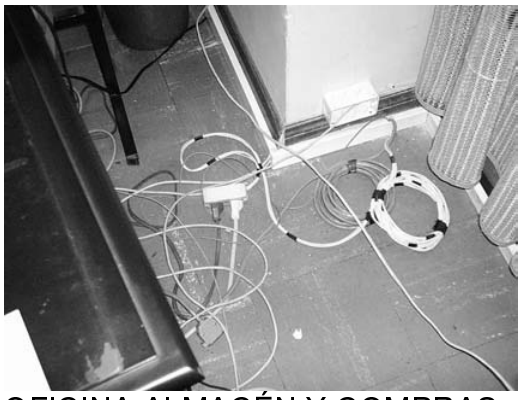
CENTRO DE INFORMÁTICA



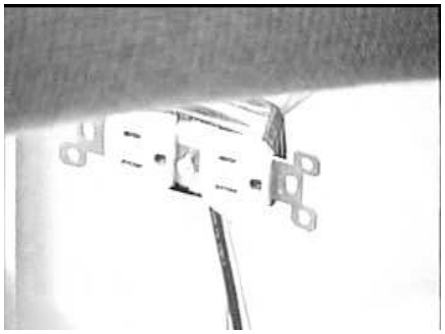
OFICINA DE ALMACÉN Y COMPRAS

SEEV07

CENTRO DE INFORMÁTICA



OFICINA ALMACÉN Y COMPRAS



OFICINA CONTABILIDAD

OFICINA TESORERÍA

SEEV08

ALMACÉN Y COMPRAS

CENTRO DE INFORMÁTICA

SEEV09

Entrevista Funcionario de Servicios Generales, Brayan Betancourt

Responsable del Mantenimiento de la Red Eléctrica de la Universidad de Nariño, Sede Torobajo

¿Cuando realizan el mantenimiento registran en alguna parte, existe algún escrito, en que notifique la realización del mantenimiento?

Por lo general servicios generales pero así que se lleve un registro no

SEEV10

Entrevista Funcionario de Servicios Generales, Brayan Betancourt
Responsable del Mantenimiento de la Red Eléctrica de la Universidad de Nariño, Sede Torobajo

¿Se hace un mantenimiento preventivo o el mantenimiento es correctivo?
Pues por la mayoría de casos que hemos tenido es correctivo.

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

19. ¿Se realiza mantenimiento a la red eléctrica?

Si generalmente estamos haciendo revisiones, casi se podría decir que no es de carácter preventivo, en la Universidad generalmente es cuando ya han ocurrido sucesos de choques eléctricos y demás, es que se ha hecho los controles, claro que lo único que hacemos aquí es revisar la UPS, que este suministrando el voltaje adecuado . - ¿Existe un encargado que revise? No, en la oficina tenemos un tester hacemos revisión de ves en cuando, también tenemos una bitácora por fechas uno va haciendo anotaciones. -¿Lo realizan Ustedes? –Si lo realizamos aquí en el Centro de Informática.

SEEV11

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 3 (Anexo ANX07)

¿Tiene un sistema de respaldo en el sentido de Planta Eléctrica?
No, no hay planta eléctrica de respaldo. ¿La Planta que tienen la Universidad en la parte de abajo? –Esta dañada, esta de adorno, creo que era solo para el Centro Administrativo que antes funcionaba allá, en el tiempo que yo estoy no la he visto funcionar .

Entrevista Realizada Programador Centro de Informática
Cuestionario No. 4 (Anexo ANX08)

21. ¿Cuentan con planta de respaldo eléctrico?

No, simplemente la oficina, tiene una UPS con capacidad de 2000.

Entrevista Funcionario de Servicios Generales, Brayan Betancourt

Responsable del Mantenimiento de la Red Eléctrica de la Universidad de Nariño, Sede Torobajo

¿El bloque administrativo cuenta con planta eléctrica de respaldo?
No, aquí ósea planta eléctrica que se maneje no.

FORMATO DE CONTROL INTERNO
EVALUACIÓN A LA RED DE DATOS DEL
CENTRO DE INFORMÁTICA DE LA
UNIVERSIDAD DE NARIÑO

EVALUACION ADMINISTRACION Y CABLEADO

OBJETIVO
Determinar el estado actual de la red de datos, teniendo en cuenta el personal a cargo, seguridad de la información seguridad en las instalaciones.

EVALUACIÓN GENERAL	**REF: SRC01** **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
ASUNTO	SI	NO	N.A	R.P.F
Administración				
Existe un responsable de las redes de comunicaciones (administrador de la red).	X			
Se tiene un diseño de la red de datos		X		SRH01
Existe un documento que especifique la ubicación de lo equipos.		X		SRH02
La red de datos es monitoreada periódicamente.				
Utilizan servidores dedicados a un solo propósito.	X			
Los servidores están protegidos por FIREWALL.	X			
El FIREWALL aisla el servidor de la intranets con los accesos de la Internet.	X			
El FIREWALL aisla el servidor de redes internas no autorizadas.	X			
El FIREWAL Registra el tráfico que sale o llega a la red privada.	X			
El FIREWALL Bloquea el tráfico no deseado.	X			
Esta restringido el acceso a los servidores.	X			
Los equipos de computo se encuentran etiquetados	X			
Los equipos de comunicaciones se encuentra en habitaciones cerradas, con acceso limitado a personas no autorizadas.		X		SRH03
Los dispositivos adquiridos cumplen con estándares de la IEEE. Según el servicio que prestan.	X			

FORMATO DE CONTROL INTERNO EVALUACIÓN A LA RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO				
EVALUACIÓN GENERAL	**REF: SRC02** **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
ASUNTO	SI	NO	N.A	R.P.F
Cableado				
Existe un centro de cableado.	X			
Cuenta con armarios para el cableado.	X			
Cuenta con paneles de conexión para organización de cables.	X			
El cableado utilizado cumple con los estándares de cableado.	X			
Las distancias utilizadas para el tendido de cables se ajustan a las especificaciones según su tipo.	X			
El cableado interno esta protegidos por canaleta		X		SRH04
el cableado externo se encuentra protegido				
El cableado se encuentra alejado o aislado de conductos o desfogues de agua	X			
Utilizan Partch Cord.		X		SRH05
El cableado se encuentra protegido por tubería, o canaleta el cableado.		X		SRH06
El ponchado de cables se adecua a los estándares establecidos por las normas.	X			
Las terminales de cableado se encuentran correctamente instaladas.		X		SRH07
Los puntos de red se encuentran debidamente etiquetados	X			
el cableado interno se encuentra instalado con canaleta	X			
La canaleta utilizada es no inflamable	X			
Las canaletas se encuentran firmemente aseguradas paredes	X			
Los puntos de red se encuentran terminados en cajas con tomas.		X		SRH08

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH01 **Fecha :** Abril/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 01	
El centro de informática no cuenta con un diseño de la red de datos. **Evidencia:** SREV01	
RECOMENDACIÓN	
El centro de informática debe contar con un diseño de la red de datos, con el fin de mejorar la efectividad en la solución de problemas de éste tipo, el diseño debe contemplar los sitios y dispositivos por donde se realiza la transmisión nombres de los puntos de origen y de los puntos de destino.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH02 **Fecha :** Abril/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 02	
No existe un documento en el que se especifique, la ubicación de los equipos. **Evidencia:** SREV02	
RECOMENDACIÓN	
Se debe generar un registro de la ubicación de los equipos, en donde se establezca información sobre, ubicación del equipo, responsable, dirección IP, red a la que pertenece, dispositivo de conexión al cual se encuentra conectado (si lo esta).	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH03 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 03	
Existen dispositivos que no se encuentran en áreas de tipo restringido, y se encuentran vulnerables a que personal mal intencionado pueda realizar daños a la red o a los mismos dispositivos. **Evidencia:** SREV03	
RECOMENDACIÓN	
La ubicación de los dispositivos de red en lugares de acceso restringido y/o protegidos por racks asegurados con llave, siendo responsable de la llave el administrador de la red de datos, y manteniendo una copia en el centro de informática.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH04 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 04	
Existen tramos de cableado que no se encuentran protegidos por canaleta o ductos. **Evidencia**: SREV04	
RECOMENDACIÓN	
Existen secciones que no se han implementado con canaleta o ductos de cableado estructurado, se recomienda realiza la protección de la totalidad del cableado, con canaleta según el trafico que exista o tubería para exteriores.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH05 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 05	
Existen Equipos que se encuentran conectados a la red de datos y que no hacen utilización de Parch Cord, realizando la conexión a la red de forma directa al cable de red. **Evidencia**: SREV05	
RECOMENDACIÓN	
Garantizar que todos los dispositivos que deban hacer uso de Parch Cord lo tengan instalado, de acuerdo a los estándares de redes de datos, ademas se debe realizar revisiones de su estado con el animo de minimizar lo problemas generados por el desgaste o daño de estos elementos.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH06 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 06	
Se encuentran sectores de cableado que no están protegidos por canaleta o ductos. **Evidencia**: SREV06	
RECOMENDACIÓN	
Se debe proteger el cableado de datos, mediante la utilización de canaletas para interiores plástico o metálica dependiendo del trafico que exista, y ductos de cableado estructurado para exteriores.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH07 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 07	
Se encuentran puntos críticos en Almacén, Ocara, Centro de Informática, Tesorería en donde se observa terminales que no generan ningún tipo de protección. **Evidencia**: SREV07	
RECOMENDACIÓN	
Proteger el Terminal de los cables, de tal manera que se encuentre aislado y correctamente ajustado a su conector.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH08 **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 08	
Los puntos de red presentan problemas en las instalaciones de las cajas, ya que en muchos de los puntos no se encuentran instaladas **Evidencia**: SREV08	
RECOMENDACIÓN	
Realizar la instalación de redes de datos estructuradas, instalando cajas de conexión en los puntos de trabajo y ajustándose a las normas de cableado estructurado.	

FORMATO DE CONTROL INTERNO
EVALUACIÓN A LA SEGURIDAD DE LA RED ELECTRICA DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO

MANTENIMIENTO DE LA RED DE DATOS

OBJETIVO

Verificar que se realicen acciones de mantenimiento a la red de datos para garantizar el buen estado y funcionamiento de la misma.

EVALUACIÓN DEL MANTENIMIENTO DE LA RED DE DATOS	**REF:** SRC03 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
		X		SRH09
El mantenimiento preventivo se realiza revisando: • Estado de limpieza. • Si hay presencia de oxido. • Si hay humedad. • Roturas. • Tornillos flojos. • Cables sueltos. • Cajas dañadas. • Jacks dañados. • Patch Cord defectuosos.			X	
Se registran los resultados de la inspección, las fallas importantes y las acciones que se ejecutan en el mantenimiento correctivo o preventivo?		X		SRH10
Las acciones de corrección se planifican de acuerdo a la importancia y urgencia de las misma?	X			
Se atienden oportunamente los problemas de los usuarios frente a problemas de redes de datos?	X			

EVALUACIÓN DEL MANTENIMIENTO DE LA RED DE DATOS	**REF:** SRC04 **Elaboró:** M.C.T y E.A.F **Fecha :** Febrero / 2004			
A S U N T O	**S**	**N**	**N.A**	**R.P.F**
Se realizan revisiones del estado del cableado para determinar si existen fallas?	X			
Se realizan las correspondientes correcciones	X			
Se remplaza equipos dañados o que estén presentando o puedan presentar problemas en las redes de datos		X		SRH11

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :** SRH09 **Fecha :** Mayo/2004,Abril/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 09	
No se realizan mantenimientos preventivos a las redes de datos. **Evidencia:** SREV09	
RECOMENDACIÓN	
Se debe realizar un mantenimiento preventivo periódico a las redes de datos, que contemple la limpieza, presencia elementos que afecten los dispositivos o medios de comunicación como oxido, humedad, corrientes eléctricas, rupturas, terminales defectuosos, cableado suelto y certificación de señales de la red.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. : SRH10** **Fecha :** Abril/2005 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 10	
Los problemas ocurridos en el mantenimiento correctivo no se documentan. **Evidencia**: SREV10	
RECOMENDACIÓN	
Se debe mantener un registro de los problemas presentados en los dispositivos y cableado, realizado un seguimiento a estos casos, y determinando posibles causas para poder tomar los correctivos necesarios y registrar la solución dada.	

EVALUACIÓN A LA SEGURIDAD RED DE DATOS DEL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO	**R.P.T. :SRH11** **Fecha :** Mayo/2004 **Realizado por :** E.A.F. y M.C.T.
HALLAZGO 11	
Se utilizan equipos que han presentado fallas y no se han podido corregir, y su operación es parcial. **Evidencia**: SREV11	
RECOMENDACIÓN	
Revisar que equipos presentan daños parciales o totales y realizar los correspondientes cambios o reposiciones, por equipos nuevos o nuevas tecnologías si fuera necesario, de ser posible su reparación, se recomienda que estos dispositivos se almacenen como dispositivos de respaldo frente a posibles daños.	

SREV01
Entrevista Realizada Programador Centro de Informática

Cuestionario No. 4 (Anexo ANX08)

¿Existe el Diseño de la red de datos?
La empresa que fue contratada para hacer el diseño de la red dejo únicamente, el cableado que hay entre el tablero y los puntos, los puntos no fueron numerados correctamente, razón por la cual debido a que de todas formas tocaba hacer la instalación de los computadores nosotros reasignamos el numero de los puntos, en el momento entonces las cajas de las oficinas tienen su numero correspondiente con el panel central.

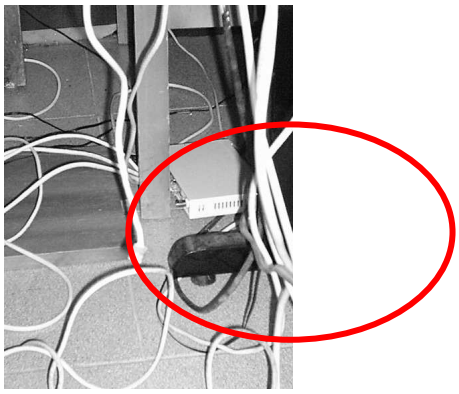
SREV02
Entrevista Realizada Programador Centro de Informática

Cuestionario No. 4 (Anexo ANX08)

¿Actualmente existe un documento en que se especifique la numeración y ubicación correspondiente de cada punto de las dependencias?
Respuesta: No, no la hemos elaborado simplemente se hace visualmente, en el momento de hacer algún mantenimiento.

SREV03

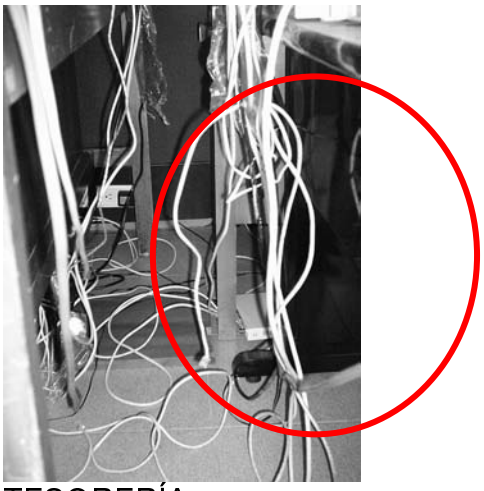
ALMACEN Y COMPRAS



TESORERIA

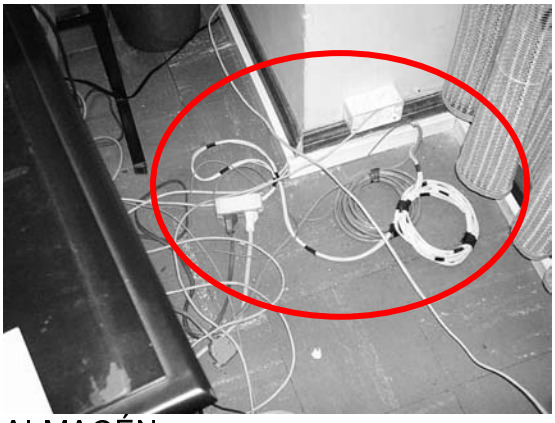
OBSERVACIONES :Equipos en el piso , equipo cerca de planta

SREV04

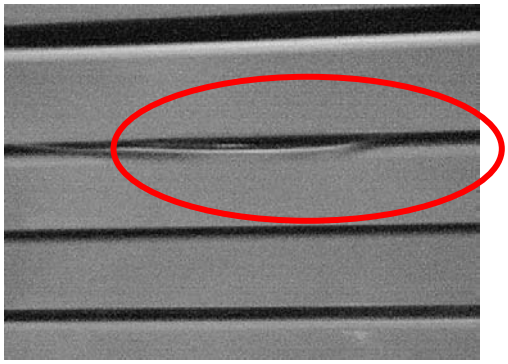


TESORERÍA

CENTRO DE INFORMÁTICA



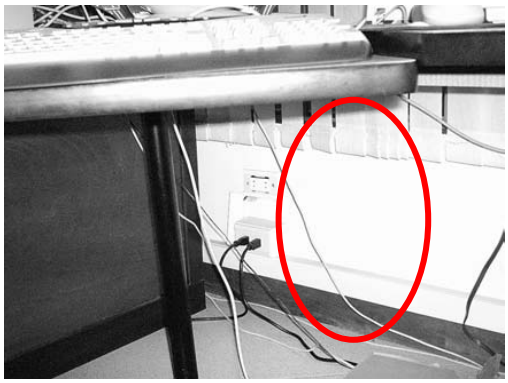
ALMACÉN



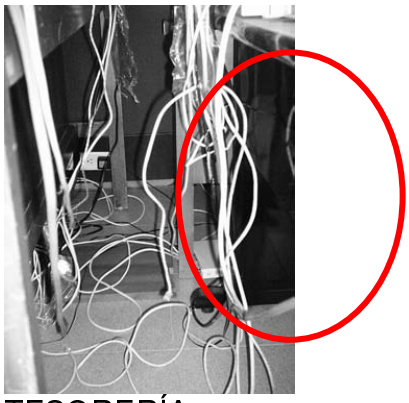
OCARA

OBSERVACIONES: Maraña de cables, entrecruce de cables de datos y corriente.

SREV05

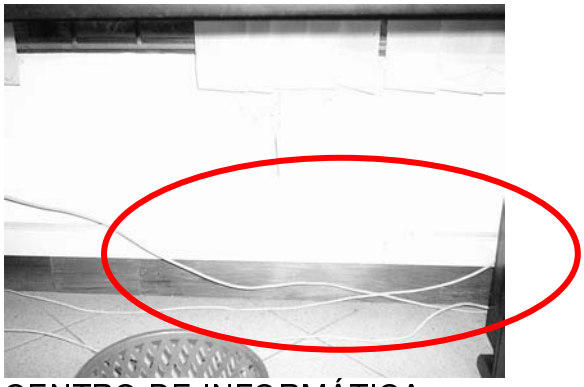


CENTRO DE INFORMÁTICA

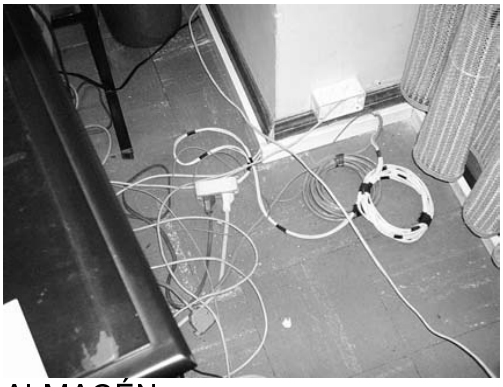


TESORERÍA

SREV06

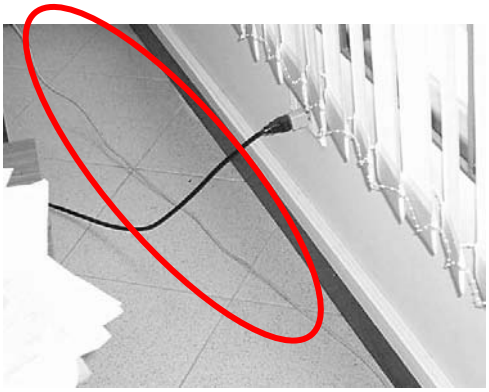


CENTRO DE INFORMÁTICA



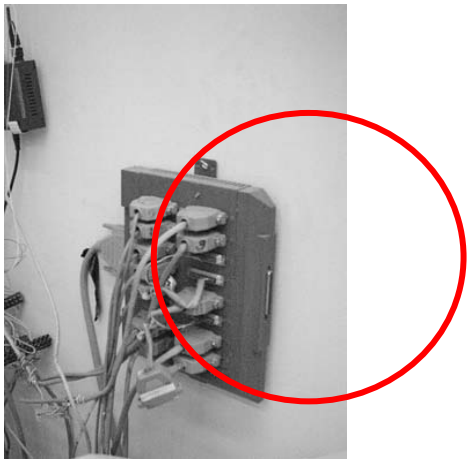
ALMACÉN

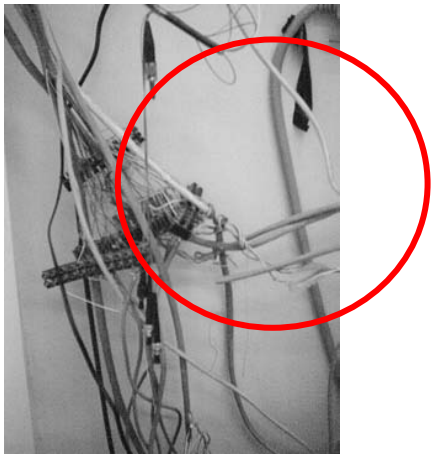
ALMACÉN



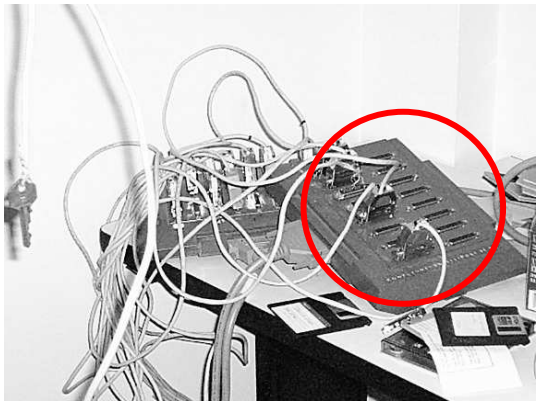
TESORERIA

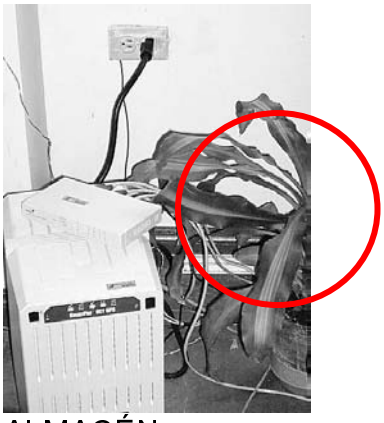
SREV07





OCARA

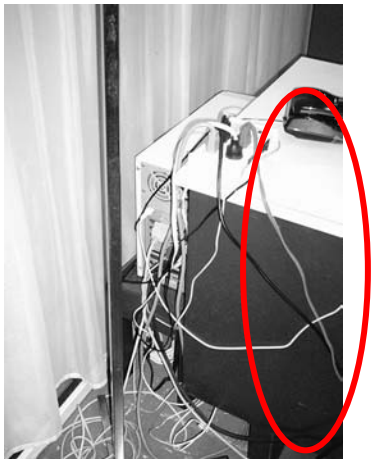




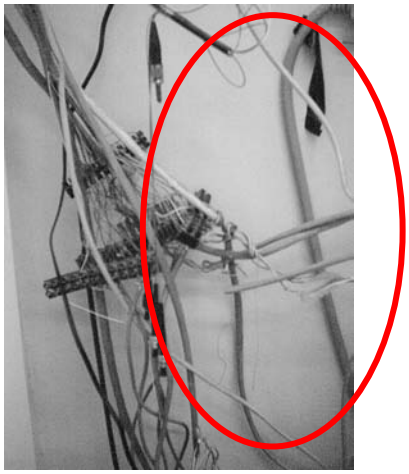
CENTRO DE INFORMÁTICA

ALMACÉN

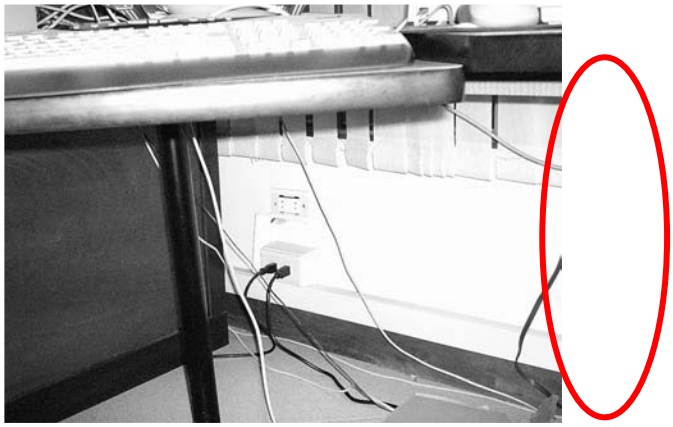
SREV08



ALMACÉN



OCARA



CENTRO DE INFORMÁTICA

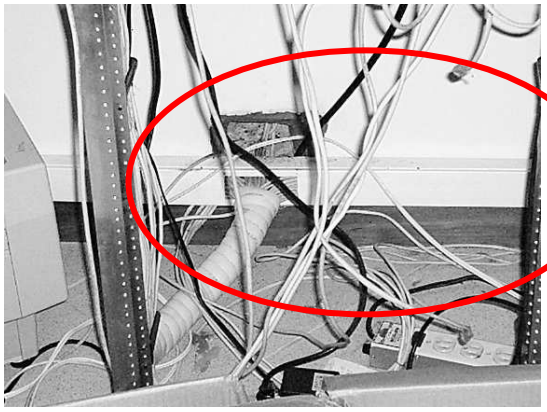
SREV09

Entrevista Realizada Programador Centro de Informática

Cuestionario No. 3 (Anexo ANX07)

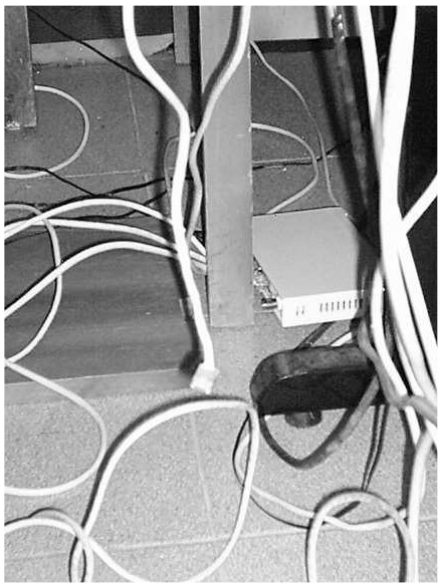
¿Se realiza mantenimiento preventivo periódico a las conexiones de la red de datos?

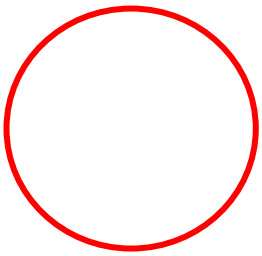
Cada vez que hay un daño.



CENTRO DE INFORMÁTICA

ALMACÉN





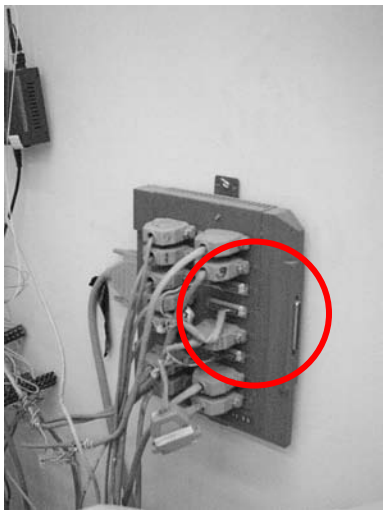
TESORERÍA

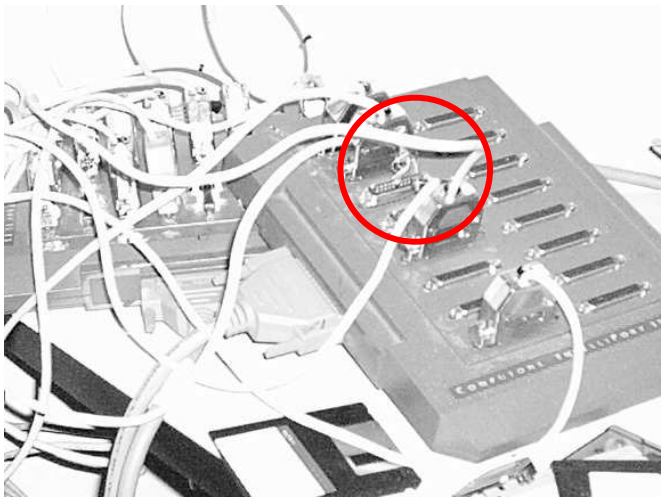
SREV10
Entrevista Realizada Programador Centro de Informática

Cuestionario No. 3 (Anexo ANX07)

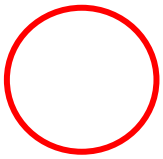
¿Se registran los resultados de la inspección, las fallas importantes y las acciones que se ejecutan en el mantenimiento correctivo o preventivo?
No, yo no he visto registro escritos.

SREV11





OCARA



CENTRO DE INFORMÁTICA

CONCLUSIONES AUDITORIA

El Centro de Informática cuenta con personal calificado para el desarrollo de las actividades que desempeñan y que han demostrado responsabilidad, alto grado de compromiso y ética, lo cual brinda cierta seguridad de que los procesos de desarrollo y administración de los sistemas de información, bases de datos programación y demás se desarrollan a conciencia y con ciertas normas de seguridad.

De igual manera se puede expresar de los funcionarios que operan los sistemas desarrollados quienes a pesar de mantener bajos niveles de seguridad respaldan con so compromiso y ética la información y programas que manejan.

Los grados de confianza y compromiso de los trabajadores son puntos a favor del sistema actual sin embargo, no son suficientes para afrontar los peligros tecnológicos con los que cuentan los sistemas de hoy en día, ni con las generaciones de estudiantes modernos, que son cada ves mas inquietos y curiosos de la los procesos sistematizados y no debemos pecar por exceso de confianza pensando que como las situaciones no se han presentado hasta ahora o que si lo han hecho no han afectado de manera significativa nunca lo van a hacer, es por eso que se deben adoptar las medidas correctivas y preventivas necesarias, seguir las recomendación y profundizar los estudios para cada ves mejorar nuestro niveles de seguridad.

De la misma manera que se deben establecer controles lógicos a los sistemas, también se debe implementar medidas de control y aseguramiento físico, por que es muy fácil hoy en día transitar con una computadora, disco duro, u otro dispositivo por cualquier rincón de la universidad, sin tener ningún tipo de restricción y sin saber cual es origen o el destino que tendrán esos dispositivos. De ahí la importancia de reforzar con personal capacitado la vigilancia y control dentro de las áreas más delicadas como el Centro de Informática.

La capacitación es uno de los pilares del mundo moderno y es la mejor manera de llegar a los trabajadores para generar en ellos la una conciencia de seguridad y crearles nuevos procedimientos que reduzcan de alguna manera las vulnerabilidades con las que cuentan es estos momentos. Además establecer que la capacitación en seguridad informática debe ser un tema constante, debido a que la tecnología esta avanzando día a día y que los procesos de seguridad deben ir a la par de esos avances.

Es por esto que el personal que desarrolla aplicaciones, presta servicios en redes, eléctricos, acceso, y hasta las mismas estructuras físicas deben estar preparadas, en constante retroalimentación y actualización para afrontar las nuevas modalidades de ataques y los nuevos riesgos tecnológicos.

Si bien en cierto los procesos de mejoramiento son necesarios y cuando hablamos de seguridad se hacen obligatorios, estos debe hacer parte de un procesos de reestructuración no solo mental sino también de tipo administrativo, quienes deben ser los primeros en tomar conciencia de la necesidad de mejorar la seguridad, y quienes deben crear los espacios y brindar los recursos económicos y de personal para lograr el objetivo que será que la seguridad llegue de manera segura a la universidad.

ANEXO B

CONTENIDO ARCHIVO PERMANENTE

CARTA DE SOLICITUD DE PLANOS Y MANUALES A PLANEACIÓN ANX01

ACTA DE ENTREGA OFICINA DE PLANEACIÓN ANX02

ENTREVISTA DIRECTOR CENTRO DE INFORMÁTICA No.1 ANX03

ENTREVISTA DIRECTOR CENTRO DE INFORMÁTICA No.2 ANX04

ENTREVISTA PROGRAMADOR CENTRO DE INFORMÁTICA No.1 ANX05

ENTREVISTA PROGRAMADOR CENTRO DE INFORMÁTICA No.2 ANX06

ENTREVISTA PROGRAMADOR CENTRO DE INFORMÁTICA No.3 ANX07

ENTREVISTA PROGRAMADOR CENTRO DE INFORMÁTICA No.4 ANX08

ENTREVISTA WEB MASTER UNIVERSIDAD DE NARIÑO ANX09

ENTREVISTA AUXILIAR DE TESORERIA ANX10

ENTREVISTA AUXILIAR DE OCARA ANX11

ENTREVISTA AUXILIAR DE ALMACÉN ANX12

ENTREVISTA AUXILIAR DE CONTABILIDAD ANX13

ACTA 006 COMITÉ DE SISTEMAS ANX14

CONCLUSIÓN ENTREVISTA COORDINADOR AULA INFORMATICA ANX15

FICHAS UNIDAD DE MANTENIMIENTO OCARA ANX16

FICHAS UNIDAD DE MANTENIMIENTO ALMACÉN ANX17

RELACIÓN SOFTWARE LICENCIADO UNIVERSIDAD DE NARIÑO ANX18

RELACIÓN LICENCIAS MICROSOFT ANX19

INVENTARIO CENTRO DE INFORMÁTICA ANX20

ACUERDO 010 DE 1986 (CREACIÓN CENTRO DE INFORMÁTICA) ANX21

RESOLUCIÓN NÚMERO 1877, 22 DE ABRIL DE 2002 ANX22
MANUAL DE FUNCIONES 2001 PARA CENTRO DE INFORMÁTICA ANX23

ENTREVISTA JEFE DE TESORERÍA ANX24

ENTREVISTA JEFE DE CONTABILIDAD ANX25

ENTREVISTA JEFE SERVICIOS GENERALES ANX26

ENTREVISTA DIRECTOR EMPRESAS DE SEGURIDAD ANX27

ESTRUCTURA ORGÁNICA UNIVERSIDAD DE NARIÑO ANX28

ANX03

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **DIRECTOR DEL CENTRO DE INFORMÁTICA**

1. ¿Hace cuánto Usted viene trabajando en el Centro de Informática?
Venimos aproximadamente, no estoy seguro, puede ser unos cinco años aquí en esta dependencia. – ¿Y los cargos que ha desempeñado dentro de la dependencia, cuales han sido durante estos cinco años? – Los cinco años ha sido de director. – ¿Ya durante estos cinco años cual ha sido la misión y la visión que se ha tenido en el centro de informática de la Universidad de Nariño? – Bueno, cuando yo recibí esta dependencia no habían, digamos en el momento definido claramente las funciones, existían unas funciones, unos procedimientos que se deberían hacer, pero no estaban digamos expresados en un manual, poco a poco lo que se ha tratado de hacer en los cinco años es ir reformando, mejorando los procesos que se adelantaban tanto en la parte académica como en la administrativa realmente pues el sistema que en el momento todavía esta funcionando tiene una serie de deficiencias en cuanto a su misma estructura a su conformación y también pues deficiencias de tipo tanto, en el software que se utiliza, como en el hardware, entonces se ha tratado en estos años de ir en el fondo como apagando incendios de las cosas que venían desde hace años atrás realmente por eso es que surgió la propuesta de reformar absolutamente todo, mejor dicho es hacer reingeniería, tomar prácticamente una partida desde cero para volver a conformar todo el sistema pues debido a todas las dificultades que se ha tenido con entidades del estado que vigilan a la universidad, hemos tenido muchísimos problemas y realmente la necesidad de reformar totalmente el sistema de información nos dimos cuenta que era una cosa sumamente urgente prioritaria para la universidad – ¿Esa seria como la misión que se tenia como la reforma? – Si, absolutamente.

2. ¿Según el acuerdo 10 del 86 que fue cuando se creo el centro de informática aquí se establecieron unos objetivos, los objetivos que se establecieron desde ese tiempo son los mismos que se ha establecido el centro de informática ahora o en que han cambiado?
Pues han cambiado digamos mucho en, digamos que los objetivos iniciales son muy parecidos a los que hay ahora, digamos que la dependencia en esa época,

en el 86, en ese tiempo la misma tecnología como también el mismo desarrollo de las mismas herramientas computacionales era demasiado, pues comparado con lo que tenemos ahora, bastante atrasado, se han ido cambiando las concepciones en cuanto a los sistemas, en tanto a tener digamos, por lo menos ahora tratar de tener un sistema distribuido que es lo que no tenemos en el momento y básicamente los cambios tecnológicos han hecho que muchos de esos objetivos se hayan ido replanteado, en esa época prácticamente la oficina de sistemas, que creo que en ese momento no se si se llamaba centro de informática, en ese entonces solamente se encargaba de hacer los procesos de nomina, se llevaba la nomina en ese tiempo en una hoja de calculo, entiendo que el Ingeniero Delio Gómez, hizo eso, estuvo trabajando con un computador y haciendo la nomina en una hoja de calculo hasta que después se adquirió un computador creo que se empezó a trabajar ya con sistemas multiusuarios, inicialmente la universidad compro el XENIX que es una versión de SCO anterior al UNIX, entonces aquí se tienen los originales de XENIX, comenzaron con XENIX y a trabajar con las primeras versiones de entonces fundamentalmente se trabajaron los procesos administrativos como el de la nomina fundamentalmente fue dedicado a la nomina y se empezó hacer algo para lo que es el registro académico, apenas en esa época y posteriormente pues se paso a otros, ya la universidad se metió con otros, plataforma UNIX, se siguió con INFORMIX y es básicamente lo que se tiene en el momento, que en el momento ya es sumamente atrasado lo que tenemos, no es un sistema que permite distribuir, es simplemente un sistema multiusuario de una sola base, no puedo relacionar base con lo que se tiene en el momento que es una gran dificultad.

3. ¿Dentro de estos objetivos hay uno que me llama la atención y dice: aportar al área académica de todos los medios y recursos para que desarrollan los programas curriculares e investigativos en los sistemas y programación a lo que se refiere?

– Claro justamente, – ¿este seria un objetivo propio del centro de informática? – No, ese objetivo se lo atribuye al aula de informática, al aula, muchas de esas cosas se partieron y muchas son manejadas por el aula de informática entonces al crearse el aula de informática digamos que se partió en 2 el manejo de los sistemas y los apoyos que pueden dar los sistemas en la vida universitaria uno que es para la gestión administrativa y otra que es para la gestión académica, en la parte administrativa hay una cosa que se comparte con lo académico que es lo de registro y control, que tiene que ver con la parte administrativa pero tiene directa relación con la parte académica por eso lo que se esta haciendo ahora en cuestión académica se lo esta compartiendo con el aula de informática ellos muchos procesos de tipo académico se los esta llevando ya para el administración del aula a través de Internet pero con una directa relación todavía el centro de informática que esta siendo parte como un puente entre los datos que aparecen en Internet y los datos que se manejan directamente en OCARA, entonces estamos trabajando es de esa manera, esa parte entonces esta compartida entre el aula de informática y el centro de informática. Pero lo de más por ejemplo la

parte netamente administrativa la maneja el centro de informática el aula toma apoyos de tipo académico a las diferentes unidades académicas, a los departamentos, a las facultades, ese objetivo por ejemplo ya es netamente del aula de informática.

4. ¿cuál es la función del comité de sistemas con el CI ?
Bueno haber en el momento el comité de sistemas es un organismo asesor que no tiene y depende del CI, no el comité de sistemas es como les dije un organismo asesor en ultimas es para el concejo de administración de la universidad en particular par el rector , eso no depende del centro de informática el director del CI hace las veces de secretario de ese comité el comité de sistemas fue creado hace algunos años pero tubo una reforma digamos que se lo recreo cambiándole su forma de operar que antiguamente estaba muy metido con la cuestión tanto con las recomendaciones técnicas como para compras sino se metía mucho con la cuestión de la ejecución de las compras, actualmente el comité de sistemas solo emite conceptos técnicos pero no tiene nada que ver con adquisiciones, con compras con absolutamente nada y solamente digamos ahora se preocupa el comité de sistemas de las políticas de desarrollo en sistemas de la universidad y es un organismo asesor, asesor de la rectoría y del consejo de administración.

5. ¿Las proyecciones que tiene el centro de informática diseñadas o planteadas a corto, mediano y largo plazo en lo que tiene referencia a la parte lógica, a la parte física y a la parte de recursos humanos, como está diseñada, como está planteada?
Haber digamos es como hacia el futuro se ha proyectado esta dependencia. Esta previsto hacer una reforma de la dependencia, esa va hacer, yo creo que a mediano plazo, con la sugerencia del comité de sistemas de hacer un replanteamiento de los sistemas de la universidad, surgió allí también la necesidad de hacer una reformulación de la composición y de las mismas funciones de esta dependencia. Pues arrancando el proyecto de conformación del nuevo sistema de información de la universidad de Nariño que arranco por la parte de digamos de los módulos de gestión administrativa y concretamente es en lo de la parte financiera, arrancando con ese proyecto se pretende también, fortalecer el centro de informática como una dependencia dentro de la universidad que, digamos, gobierne los sistemas y su desarrollo internamente, dejando al aula de informática lo correspondiente al soporte físico, que serian las redes, la intranet, el aula de informática manejaría el soporte físico y el centro de informática haría el soporte lógico de los sistemas de la universidad, entonces primero el comité de sistemas detecto que la oficina en el momento, primero que tiene muy escaso personal, nosotros hemos visitado otras universidades y por ponerles un ejemplo la universidad de Pamplona, la oficina de sistemas tiene aproximadamente 25 ingenieros de planta que hacen desarrollo, mantenimiento, soporte técnico, soporte funcional en cuanto a los paquetes que ellos producen, capacitación, es eso aquí realmente hay 2 ingenieros y 2 programadores, para una universidad de pronto mas grande que la de Pamplona, entonces el comité de sistemas se dio

cuenta primero el recurso humano, la oficina tiene unas grandes deficiencias, segundo que no hay una organización como dependencia de sistemas por decir algo aquí debería haber ingenieros trabajando en diferentes áreas, por ejemplo debe haber un ingeniero trabajando solo en seguridad, debería haber un ingeniero solo por ejemplo en mantenimiento y soporte a las bases debería haber unos ingenieros como analistas deberían haber unos programadores, hace falta, primero en personal muy mal segundo se debe hacer una reorganización y crear unos cargos dentro de la dependencia en el momento no lo hay simplemente aquí el director delega funciones a los cuatro funcionarios que están aquí claro que se los ha ubicado en algunas áreas pero todo se hace por delegación, es decir que la reforma se va hacer a mediano plazo.
En la parte física hay otra cuestión la reforma incluye, por ejemplo nosotros en el momento estamos trabajando con 2 servidores que básicamente son Pc´s como medio mejoraditos con discos duros scocí con unas boards buenas, memoria bueno pero realmente eso no es para mantener los datos que nosotros tenemos, entonces la universidad ya por lo menos para el CI compro una estación sun blade 2000 que es de las ultimas que saco la sun de los perfiles mas bajitos por el costo, que costo como 44 millones y ese es de los perfiles mas bajitos que saco la sun eso es un solo procesadorcito , pero si se están haciendo los tendidos de fibra óptica que vamos a necesitar se están haciendo…. Se pretende que este año se compre la otra estación sun para aquí para el centro que sirva para respaldo de la otra que sirva de espejo si se ha pensado en hacer la formulación de esto, lo otro nosotros tenemos deficiencias físicas en cuanto a la seguridad… digamos aquí no tenemos una seguridad física … bueno no solo nosotros sino todo el edificio busque un extintor y no encuentra uno tenemos muchas fallas en la cuestión eléctrica del edificio y lo otro la seguridad contra cualquier tipo de cosas robos o lo que sea, no hay una seguridad… también se esta pensando en eso y de pronto esta oficina tendrá que trasladarse o hacer otra cosa netamente para una oficina así… pues realmente la información que se maneja aquí es la información de toda la universidad y es una cosa que es muy valiosa y ahora como va a estar cableada toda la universidad con fibra entre bloques, entonces no habría problema que nos traslademos otra parte donde se tenga una seguridad mucho mas fuerte.
– ¿Pues nos ha comentado que los recursos técnicos y humanos son escasos? – Son escasos – ¿Y los recursos económicos que recibe el centro de informática por parte de la universidad también están dentro de ese rango de escasos? – Realmente digamos el centro de informática no tiene un rubro para hacer sus adquisiciones en cuanto a hardware o software, realmente eso esta manejado directamente por la vicerrectoria administrativa en unos rubros que son generales para toda la universidad, unos rubros para la adquisición de equipos y así, pero directamente el centro de informática no tiene dinero para hacer el soporte de sus desarrollos, en ese caso es el comité de sistemas quien hace las recomendaciones al consejo de administraciones para que se hagan las dotaciones correspondientes, pero eso esta muy limitado pues al presupuesto de la universidad, por ponerles un ejemplo creo que para el desarrollo de la intranet en la universidad tenemos ciento treinta millones, pero si una estacioncita de esas

vale cuarenta y cinco sin contar software, por eso es que digamos que la propuesta que hizo el comité de sistemas es que el desarrollo del sistema de información de la universidad se debe hacer sobre el **software link** se escogió como motor para las bases **postgres** y se va hacer como el sistema que se pretende que va a estar orientado a la web, se va a trabajarlo con PHP, salvo algunas aplicaciones que requieran ciertos niveles de seguridad se las va a trabajar con aplicaciones compiladas, entonces eso ya se esta trabajando directamente sobre eso precisamente por la escasez de recursos que tiene la universidad y pues realmente por los escasos dineros que la misma universidad le dedica a los sistemas, porque pues en noviembre del año pasado, casi todos los noviembres de todos los años, se planea el presupuesto para el siguiente año en esa planeación la oficina acá de planeación, le pone valores a los rubros, entonces dicen por ejemplo para el desarrollo de sistemas y redes tantos millones, ellos pues son los que se encargan de distribuir todo el dinero, a criterio de ellos pusieron ciento treinta millones y eso es para todo el año y se supone que con eso se debe hacer todo, lo de aquí lo de otras dependencias, lo que tenga que hacerse, los recursos son escasos y el centro de informática directamente no tiene un peso. – ¿Y esta encases en los rubros usted lo ve como un nivel bastante, digamos que obstruye la consecución de los objetivos que tiene el centro de informática o que pueda tener el centro de informática? – Como – Miramos que los rubros son pocos, ¿cierto?, o que los distribuyen entre el presupuesto de la universidad, ¿esto en algún momento se vuelve un obstáculo para el cumplimiento de los objetivos o se ha convertido en el pasado en algún obstáculo para el cumplimiento de los objetivos del centro de informática? – En el pasado si ha sido un problema, en el pasado ha sido un problema no tener unos recursos propios porque digamos las directivas universitarias no le han visto mucha necesidad de fortalecer esta área, imagino por desconocimiento, donde pues radica básicamente yo creo que el 80% del funcionamiento de la universidad, ellos nunca le han visto digamos la prioridad de tener digamos esta área al día y bien equipada, bien dotada, con buen personal, eso desde el año pasado lo ha notado el comité de sistemas y se ha propuesto ha si el centro de informática no tenga un rubro directo para hacer sus compras, para hacer sus adquisiciones de manera directa, pero si apoyándolo en el sentido en que las directivas de los rubros que se han destinado para el desarrollo de los sistemas de la universidad se tenga digamos en cuenta la modernización del centro de informática, eso si esta contemplado como recomendación del comité de sistemas a las directivas, pero pues si fue una dificultad en años pasados que realmente como ponerles un ejemplo nosotros hace unos cinco, seis años estábamos trabajando con dos servidores que eran unos 4-86, dos equipos 4-86 y rato menos pensado una secretaria que era no me acuerdo que era la secretaría del departamento de filosofía pidió un computador y le compraron en esa época fue un **Acer spair**, eran los primeros que salieron negritos eran Pentium, entonces nosotros decíamos caramba nosotros con esa pobreza y la secretaría haciendo cartas con semejante, en esa época era un computadorzote, entonces no había realmente un criterio para decir mire pues a ellos hay que comprarles determinados equipos, hay que

modernizarlos, en épocas pasadas si hubo mucha dificultad porque realmente como le digo las directivas no lo veían como prioritario apoyar esa dependencia la miraban como una dependencia más, que si han venido funcionando pues han de seguir funcionando, eso era el problema que teníamos antes.

6. ¿Hablando de la estructura que tiene internamente aquí el centro de informática en cuanto a personal, cual es la organización que tiene en cuanto a los puestos de trabajo?

En este momento las 4 personas que trabajan aquí, los 4 digamos tienen funciones de analistas y programadores, los 4 desempeñan las mismas funciones, cada uno dedicado a diferentes áreas, por ejemplo Lucho Rosero, él esta encargado tanto del análisis y la programación de todo lo que tenga que ver nomina y tesorería, entonces se encarga de eso y las mismas funciones las cumple por ejemplo Henry Rodríguez él trabaja en dos frentes, un frente que tiene que ver la parte académica, en cuanto a lo que es la cartera, las deudas de los estudiantes y otra parte con la parte administrativa controlando lo que es de almacén, Freddy Portilla, él tiene también dos frentes, uno es la parte administrativa él maneja mucho lo que es presupuesto y contabilidad, combinado con unas tareas en la parte académica y Luis Carlos Estrada netamente dedicado a la parte académica, lo que pasa es que Luis Carlos su trabajo de grado desarrollo unos módulos para OCARA básicamente fue el módulo que le calcula, digámoslo así a los estudiantes su matricula para el semestre siguiente, haciéndole el análisis de todas las materias que él ha visto con sus requisitos, prerrequisitos, de acuerdo con el plan de estudios, porque pueden haber muchos estudiantes en un semestre con diferentes planes de estudios; él hizo ese desarrollo, entonces él ahora esta dedicado netamente solo a eso. Esa digamos es la distribución, pero todos hacen labores de análisis y desarrollo.

7. ¿Sus funciones como director?

Yo estaba mirando estas que me han escrito aquí, si esta, la primera esta correcta la de coadyuvar en la formulación de políticas y en la determinación de planes y programas del área, esta si esta correcta porque esta simplemente la palabra coadyuvar, porque como soy miembro del comité de sistemas, o mejor dicho el director de sistemas es miembro del comité de sistemas, entonces esta función la cumple llevando esas políticas de desarrollo, llevándolas al comité, por ejemplo esta, dirigir, supervisar, promover y participar en los estudios e investigaciones que permitan mejorar la prestación de los servicios a cargo de su dependencia, eso si es una función que digamos tiene que ser de manera evidente.

Funciones que no debe hacer que tal personal necesita un computador, que en la VIPRI necesitan un aula con red entonces incluso se metía con cotizaciones

Este fue del 2002 DEL 21 DE ABRIL ESA ES LA RESOLUCION DE LA CREACION DEL

Es simplemente una reforma que se le hace al comité de sistemas, el articulo 1ro dice por quien estará conformado el comité, la 2da actuara como secretario el director del centro de informática.

Las regulaciones o recomendaciones que el comité produzca son de obligatorio cumplimiento por todas las dependencias de la universidad y las funciones, determinar las políticas de desarrollo y redes de la universidad es el comité quien determina eso, no el director del centro de informática.
Por ejemplo el comité, es emitir conceptos e ideas sobre proyectos desarrollo de las aplicaciones informáticas o de redes para la universidad para realizarse mediante trabajos de grado , cuando se va hacer una pasantia por ejemplo dicen vamos a sistematizar no se que cosa entonces el comité tiene que dar un concepto sobre eso por que aquí se han hecho muchos trabajos de grado como por ejemplo : trabajo de grado para sistematizar las hojas de vida de los profesores de la universidad llego, hizo ese trabajo y no le preguntó a nadie y lo hizo en fox y de que nos sirve a nosotros que lo haga en fox, es por eso que al comité le ponen ese tipo de funciones
– ¿Generar políticas de seguridad, eso también es de comité de sistemas y si a cumplido el comité con esa función de definir políticas? – Lo primero que se hizo fue el replanteamiento del sistema de gestión administrativa que comenzó con la parte financiera esta también el lo de la red física de la universidad se consiguieron los recurso se paso un proyecto al ICFES se saco una plata de ese proyecto unos ochenta millones, con eso se esta haciendo los tendidos de fibra óptica, se compraron los equipos de comunicaciones se compraron dos estaciones sun una para el CI otra para el aula de informática. Con esos recursos se esta haciendo eso, sobre políticas de seguridad todavía no se ha tocado eso pero es una cosa que viene con el mismo desarrollo de los sistemas con el que se esta haciendo no se puede hacerlo el sistema y después la seguridad. – ¿Diseñar las redes de alimentación las diferentes dependencias de la Universidad …. Redes de alimentación… me imagino que sean redes de datos….? – Realmente… Esto es para el comité de sistemas la 3ra función, determinar las políticas de las redes y sistemas de la U bueno esta parte a pesar que las políticas es del comité de sistemas el desarrollo e implementación esta a cargo del aula de informática.
– ¿Digamos ahora el aula de informática es la que gobierna la intranet de la universidad y entonces se entiende con todo eso con el soporte lógico y el soporte físico? – A ellos el comité se les hizo la sugerencia que adquirieran todo el kit para fibra, incluso se lo capacito a Juan Carlos Castillo en ese sentido en todo lo que tenga que ver con conexiones de fibra entonces el esta haciendo realmente eso el hace parte del aula. – ¿Esta tampoco esta es del aula, la quinta que tiene aquí? – Dirigir el comité técnico de sistemas tampoco, por que simplemente es ser secretario del comité de sistemas quien dirige el comité de sistemas es el rector o el delegado quien lo presidirá que en este momento es el Dr. Edgar Osejo. La séptima realizar las funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo, correcto esa si esta bien

8. ¿Usted por que cree que existe esa discordancia entre lo que dice el manual de funciones de la universidad y lo que realmente es?
Yo realmente no voy a echarle la culpa a nadie pero me parece que quienes levantaron este manual no tuvieron en cuenta la resolución que crea el comité de

sistemas asignándole las funciones entonces realmente hay unas funciones que son del comité de sistemas que el comité las hace a manera de propuestas o políticas pero quien ejecutaría algunas de esas políticas es el director.
Dirigir, supervisar y promover y participar en los estudios que permitan mejorar la prestación de los servicios de la dependencia, esta bien, yo la resumiría en dar cumplimiento a las disposiciones del comité de sistemas en cuanto investigaciones que permitan mejorar la prestación de servicios de la dependencia.

ANX04

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 2

CARGO: **DIRECTOR DEL CENTRO DE INFORMÁTICA**

1. ¿Cuándo fue la construcción del bloque administrativo, donde se localiza el Centro de Informática, fueron consideradas opiniones o sugerencias de parte suya?¿Cuáles?
Sí, se hicieron sugerencias sobre todo en ductería que se debería utilizar para el cableado del Centro de Informática y del edificio, pero no fueron atendidas.

2. ¿Participó Usted en el diseño y asignación de espacios dentro del Centro de Informática?
No

3. ¿Qué parámetros tuvieron en cuenta para la distribución de áreas dentro del Centro de Informática?
Solamente hicieron la solicitud de la información de cuantos eran los funcionarios que trabajan en el Centro de Informática y si se necesitaba una especia de bodega para almacenar algunos elementos.

4. ¿Considera que el espacio que se dispone es suficiente para albergar todos los equipos de informática?
No, el espacio no es el suficiente para todas las necesidades del Centro de Informática.

5. ¿Se encuentra un lugar exclusivo y aislado para el almacenamiento de papelería?
Si hay una bodega para almacenar elementos de papelería.

6. ¿Se encuentra establecida un área para el mantenimiento de equipos?
No hay un área para el mantenimiento de equipos de hecho no se necesita pero no hay el espacio disponible.

7. ¿Existe un lugar asignado para el almacenamiento de discos y cintas?
Las cintas y discos se las mantiene dentro de los cubículos de la oficina a excepción de las cintas que se sacan de la universidad para tener un respaldo exterior de datos.

8. ¿Se tiene un área exclusiva para reuniones de oficina?
El área de reuniones es simplemente el área que hay en la oficina de la dirección del Centro de Informática.

9. ¿Se tiene un área exclusiva para equipo de protección eléctrica?
Los equipos de protección eléctrica están por fuera del centro de informática en una ubicación cercana pero aislada de las demás oficinas donde se almacenan las UPS, las baterías y lo que tiene que ver con toda la switchería del edificio.

10. ¿Se provee de un lugar para la bóveda de seguridad, altamente protegido?
No existe dentro de la universidad ni en particular en el Centro de Informática lugar para una bóveda de seguridad.

11. ¿Existe un lugar asignado para el almacenamiento de equipos fuera de uso?
Los equipos que quedan fuera de uso simplemente se dan de baja y no hay un lugar designado para este almacenamiento.

12. ¿Se mantiene algún control de temperatura y de humedad?¿Se realiza de manera constante?

No se hace control de temperatura y humedad tanto en el Centro de Informática como en el área donde se presta los servicios de comunicaciones e Internet, de hecho se hizo la solicitud de una unidad de aire acondicionado par el área donde están los servidores, pero esta petición no ha sido atendida hasta el momento.

13. ¿El uso de cigarrillo está prohibido dentro del área del Centro de Informática?

Sí.

14. ¿El departamento de bomberos ha sido informado previamente de las características y vulnerabilidades del Centro de Informática?
No, de hecho ninguna dependencia en la Universidad ha hecho este tipo de peticiones.

15. ¿Existen pólizas de seguros que cubran el riesgo y la cuantía en casos de siniestros?
Entiendo que la Universidad tiene algunas pólizas de seguros que cubren los equipos que la Universidad posee.

16. ¿Se tiene una lista actualizada de las personas con autorización de acceso permanente?
Las personas autorizadas de acceso permanente son los funcionarios del Centro de Informática, pero eventualmente acceden otros tipos de funcionarios de la Universidad por diversas razones, razones que tienen que ver directamente con los servicios que presta el Centro de Informática.

17. ¿Se tiene un control de acceso a la entrada del Centro de Informática, anotando los datos y motivo del visitante?
No.

18. ¿Se toman las medidas de seguridad adecuadas después que los empleados han terminado sus contratos de trabajo?
No, sería muy bueno que se hicieran sugerencias sobre este asunto.

19. ¿Se lleva un registro de la circulación de equipos dentro del edificio donde se encuentra el CI?
No

20. ¿Se cuenta con los equipos suficientes?
No se cuenta con los equipos suficientes, de hecho se necesitan unos tres servidores adicionales a los que ya existen.

21. ¿Se prohíbe el consumo de bebidas y comestibles en el área de cómputo?
No

22. ¿Se tiene computador de respaldo en caso de siniestros?
No se tiene computador de respaldo por esa razón es que dije anteriormente que los equipos no son suficientes y se necesitan tres servidores adicionales a los que ya se tiene

23. ¿Se lleva un inventario actualizado de equipos?
El inventario sí está actualizado.

24. ¿Se tiene identificado las características de hardware y sus capacidades?
Sí.

25. ¿Se tiene una lista del personal encargado de los equipos?
No, los equipos digamos están a cargo según el inventario en cabeza del director del Centro de Informática, pero se coordina el manejo y mantenimiento de esos equipos a personal de aquí mismo del Centro.
26. ¿Se mantiene registro de las fallas en los dispositivos de los equipos?
No

27. ¿Se realiza mantenimiento de los equipos periódicamente?
Sí.

28. ¿Se mantiene un registro de los mantenimientos practicados?
No

29. ¿Qué se hace con los equipos en desuso?
Los equipos de dan de baja y se llevan al almacén

ANX05

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: PROGRAMADOR

1. ¿Las funciones que Usted realiza dentro del Centro de Informática, corresponden a las establecidas en el manual de funciones de la Universidad de Nariño?
Sí, es correcto respecto lo que aparece acá respecto al análisis de requisitos, la creación de programas y también los mantenimientos que se le hacen al sistema operativo están incluidos acá. – ¿Adicional a las funciones que están ahí realiza otras funciones, le corresponderían funciones como las del analista? – Si es casi, estaríamos mezclando las dos. – ¿usted tenia conocimiento de estos manuales? – No – ¿Ni entre lo oficial y no oficial? – No.

2. ¿Cuando se le delega funciones adicionales, quien las asigna?
El jefe del centro de informática el es el encargado de asignar las funciones extras o las operaciones que tengan que hacerse – ¿El director esta controlando el desarrollo de las mismas? – Si, él esta controlando esas circunstancias, de acuerdo las solicititudes que hagan las dependencias entonces lo entrega por escrito o verbal y nosotros hacemos los procedimientos, los programas y cuando se hace la entrega se le avisa se le oficializa que ya se hizo la entrega a cualquiera de las oficinas.

3. En lo referente a su cargo ¿Cómo se controla?,
– ¿Acceso a las instalaciones?, A la oficina tenemos horarios establecidos, tenemos la llave – ¿Todos tienen la llave? – Solo nosotros – ¿ni los celadores ni el conserje? – nada, solo nosotros. – ¿Cuándo necesita acceder en horarios extraordinarios de trabajo el permiso lo asigna el director? – No, a veces en vacaciones toca pedir permiso a la jefe de servicios generales porque no deja entrar a la universidad, entonces el jefe hace un oficio que tenemos que venir a trabajar, ella autoriza y con ese documento escrito podemos entrar a trabajar – ¿por ejemplo un día domingo tiene problema? – Se le avisa al jefe.

– ¿Acceso a los equipos? – hay claves para cada uno de los equipos, a este me toco quitarle la clave, pero paso una vez que yo me fui y tenían que imprimir liquidaciones y no pudo, entonces me dijo quítele la clave.
– ¿Cada funcionario tiene la restricción de utilizar solo su equipo y responsabilizarse de el? – Si, cada funcionario tiene su equipo.
– ¿En lo que se refiere al acceso los programas a las aplicaciones ustedes tiene acceso solo a las aplicaciones que le corresponden? – Nosotros tenemos la condición de administrador el sistema de superusuario, con la clave del superusuario puedo entrar a cualquier programa, hay unas claves par cada programa yo tengo las claves de superusuario de contabilidad, de Tesorería, de Almacén, de Nómina, no tengo pero como soy superusuario puedo entrar – ¿los demás usuarios también manejan las claves? – Si, las conocemos es importante si no esta el compañero alguna circunstancia donde se ausente o toca solucionar un problemas entonces uno entra a uno que no este el otro. – ¿Ustedes que restricciones tienen para el manejo de equipos es decir ustedes solo lo utilizan para labores del centro de informática o también para actividades propias, pueden mover los equipos? – No, solo para los equipos no se mueven y son para actividades que se nos encomienda, tenemos el acceso a los programas, a Internet, a correo electrónico, pero pues las labores son puramente técnicas, orientadas al trabajo entonces bajamos de Internet programas técnicos para solventar las necesidades de la oficina. – ¿El acceso al cuarto de maquinas es restringido o todos pueden entrar? – Allá solo los del centro de informática, no puede entrar nadie más.

4. ¿Cómo y quiénes definen las políticas para el desempeño de su cargo?
El jefe determina, si hay una orden de parte de el de lo que se puede y no se puede hacer si los equipos o impresoras toca llevarlos a otra oficina entonces se le avisa a él, es el conducto regular para utilizar los equipos.

5. ¿Las mencionadas políticas se encuentran definidas por escrito?
No por escrito no he encontrado algo que este así, pero las establece el jefe de la oficina.

6. ¿Son suficientes los recursos asignados para el cumplimiento de sus funciones?
Ahorita si, es que esto es nuevo, aquí me siento bien chévere, buen equipo, son nuevos.

7. ¿Con qué áreas y personas se encuentra relacionado su cargo?
Con que oficinas, con la gente de contabilidad, almacén y suministros en almacén están todos los funcionario, el que maneja inventario, cardex, bodega, cotizaciones con el jefe con ellos, en contabilidad con la auxiliar contable Ali con casi todos por que hay cuestiones de matricula que se pasan a contabilidad a veces hay cosas que toca revisar o piden informes, con OCARA también la parte de liquidaciones de matricula.

8. ¿De que áreas y personas recibe información para procesamiento, con que frecuencia y bajo que procedimiento?¿De qué manera recibe la información (en línea, archivos planos, medios magnéticos, por escrito, etc) de las mismas?
De las mismas, casi permanente – ¿con almacén están en línea? – No, lo hacemos a través de archivos en cinta – ¿cada cuanto recogen la información allá? – Cada semana,– ¿Que día? – El día que se requiera hacer informes, – ¿informes semanales? – Mensuales – ¿Hay algún procedimiento? – la señora hace copia cada semana y como cada mes toca hacer un balance voy a traer esa cinta o voy con mi cinta y la copio. – ¿Eso entra a través de archivos planos? – Se copia la base de datos – ¿Y con el resto de dependencias? – Es en línea.

9. ¿A qué áreas reporta información procesada?
A todos los anteriores, a Planeacion, vicerectoria, a control interno, contraloría, a veces a las facultades – ¿Con que frecuencia, mensuales? – Mensuales, es la frecuencia de entrega de informes.

10. ¿De qué manera envía la información?
De forma escrita

11. ¿Se da cumplimiento al calendario de actividades que se tiene establecido dentro del Centro de Informática, para el envió y recepción de documentos e información?
Almacén o planeación ponen fechas, no hay oficial ellos llaman necesitamos el informe de impresoras que se compraron en la universidad y lo necesitamos para pasado, necesitamos el informe de matriculas de 2003 para tres días o mas urgentes así.

12. ¿Qué medidas de seguridad se tienen establecidas para la transmisión y recepción de datos?
La confianza que les entrego los datos y que están bien o se coloca una nota de recibido se coloca esto.... así es la forma.

13. ¿Qué problemas ha tenido?
Si, si sucede en que ellos dicen que los datos tiene errores uno lo que dice es que, reportarme ellos avisan, uno trata de conocer todo el procedimiento pero hay cosas muy técnicas. – ¿Cada cuanto revisan? – permanentemente, ese es su deber que sea coherente los datos bien calculados los nombres bien o sino tienen que informar que el software esta calculando mal.

14. En el desarrollo de sus actividades, ¿Qué problemas ha tenido en lo referente a: Red de datos, Red eléctrica, Usuarios, Acceso de intrusos, Instalaciones físicas, Otra?

¿Que se hayan metido a la red? – La red interna esta aislada, – ¿por Internet no hay posibilidad? – La cuestión es que lo que se entrega a Internet son archivos, el enlace a la base de datos física no se puede esta separado lo que nosotros hacemos generar un archivo de texto plano copiárselo allá al sistema de información de intet y luego lo suben no hay un vinculo de base de datos, hay una especie de triangulación que físicamente no permite comunicarse. – ¿Los computadores de aquí están conectados directamente al servidor? – Si – ¿Ha tenido problemas de perdida de información? – No, yo saco varias copias de las tablas – ¿cada cuanto saca copia? – A diario, hay un procedimiento que es automático donde se sacan cintas todos los días.

15. ¿Describa brevemente las actividades y procedimientos que realiza diariamente en el centro de informática?

Llego, pues lo que se hace aquí es realizar programas, mantenimiento de los mismos, hacer informes, reportes y atender a los usuarios de nosotros atendemos a nuestros usuarios de los sistemas nuestros. Ahorita tengo que instalar un inventario para el sistema de librería, estuve sacando un informe de matriculas, de cartera, de deudores. Instalarle al encargado de cartera programas que el pidió. – ¿Quién realiza el control sobre estas actividades?
– El jefe y los usuarios si no entregue el programa ya le dicen a el, toca entregarle rápido para que no se quejen.

16. ¿Que actividades realiza periódicamente?

Cada tres meses hacer un informe a la contraloría, la contraloría pide cada tres meses lo que la u ha gastado la u paga profesores paga insumos compra equipos de laboratorio, eso se ve reflejado en el paquete de almacén, tesorería, contabilidad y presupuesto, toca cruzar los cuatro paquetes – ¿Ese cruce de información se hace en línea o manual? – Se hace manual por que el sistema no esta integrado se hace en Excel, entonces yo cada tres meses se acaba el primero de marzo el primero de abril debe estar listo y los otros 15 días el encargado, hay un contador que lo revisa lo firma y lo entrega, quemas, las cuestiones de liquidación de matricula, genero recibos de matricula cada seis meses, un mes antes me toca cuadrar eso que implica cuadrar eso que hay deudores, extraordinarias cuotas, descuentos, intereses, reclamos, yo reviso todo eso para depurar hay funcionario allá que se encarga de eso pero hay cosas que hay que hacer por Software, actualizaciones, que se va poder actualizar 2000 estudiantes habiendo un programa que hace eso, tres semanas hago eso en una semana miro mas o menos el archivo de impresión en tres días imprimo al otro se entrega y las dos semanas siguientes para reclamos, ahorita en marzo me toca imprimir las segundas y terceras cuotas los bancos reportan lo que pagaron los estudiantes esos reportes lo subimos al sistema, actualizamos deudas y sabemos que se esta debiendo – ¿Quiénes reciben esos estratos? – Nosotros por Internet por medio de correo electrónico entre Freddy y mi persona lo hacemos, informes de inventarios estadísticos pide el vicerrector – ¿esos informes son eventualmente o son en la misma

fecha? – El siempre pide cosa y toca sacarle, Planeación también pide, el jefe de almacén, control interno, auditoria, hay un proceso de notas que periódicamente hay un registro académico de notas académicas de notas antiguas en cada facultad, los usuarios los digitan yo las traigo aquí y las subo al sistema.
– ¿Usted dice que realiza copias de seguridad diariamente, en que medio se realiza? – En cinta – ¿siempre las realiza en cinta? – Si, en cintas de ocho Gigas hay una imagen también como hay dos servidores es una replica un espejo entonces lo que tiene el sistema de gestión esta en OCARA y OCARA en gestión – ¿En dónde se almacenan las copias de seguridad? – Las tiene Freddy – ¿Quiénes tienen acceso? – Nosotros, las guarda en una gaveta ahí esta echado llave, el tiene la llave – ¿Existen copias de seguridad fuera de la Universidad? – El jefe a veces periódicamente las saca y se las lleva – ¿en la casa las tiene? – Si – ¿y allá quienes tienen acceso? – Pues el esta en su casa no hay nada que hacer. – ¿Frente al desarrollo de software, usted qué metodología de desarrollo utiliza? – El normalito, es el espiral, análisis, analizo, diseño, programo instalo, pruebo y vuelve y juega analizo, diseño, tas, tas es un modelo incremental. – ¿Se documenta la información de análisis y diseño? – Documentar, documentar oficialmente no, con todos los diagramas no, no ahí no cabe, no – ¿Pero si existe un análisis, un diseño? – si claro.

17. ¿Quiénes realizan el control y aprobación de los procesos de análisis, diseño o desarrollo, y lo aprueban?
Los usuarios, ellos revisan si esta bien el producto, formalmente no hay quien lo apruebe cada uno es responsable de que funcione.

18. ¿Qué medidas de seguridad implementa dentro de las aplicaciones que ha desarrollado?
Validaciones de todo tipo – ¿hay un control a los usuarios? – Contraseñas – ¿registro de actividades tiene? – Si de algunas, si hay, a la hora en que mete el dato el usuario – ¿ellos pueden realizar procesos de eliminación, modificar? – Eliminar, si pueden pero cuando eliminan yo cargo en otra tabla, nunca se borra, jamás por que después reclaman que por que se borra ya me ha pasado – ¿y cuando modifican? – también eso esta en otra tabla, cada año hago replicas – ¿durante cuanto tiempo se guardan estos registros? – Desde que yo entre ahí están – ¿cada cuanto revisan? – yo reviso, los inventarios se revisan cada seis meses, el procedimiento de inventario es corregir aquellos artículos que ya están dañados, adicionar se adicionan automáticamente cuando se compran pero a veces cambian de dueño entonces ahí ya registra eso, como dos veces en el año se hace copia de eso.

19. ¿Cada cuánto se realiza cambio de contraseñas de los usuarios?
Cada vez que ellos digan, ellos definen eso. – ¿Cada usuario tiene nombre de usuario y contraseña? – Si cada uno tiene su clave, tiene permisos de

ejecución para los programas – ¿Usted asigna los permiso? – Si, digamos que si uno tiene acceso a inventario otro a cardes.

20. ¿Dentro de sus actividades y responsabilidades ha establecido planes de contingencia frente a posibles percances?
No, no hay.

21. ¿Conoce los procedimientos a seguir frente a posibles desastres? (incendios, inundaciones, terremotos, disturbios)
Salir corriendo, los equipos ahí cualquier cosa se hace de algunas cosa tengo copia en mi casa.

22. ¿Ha participado de simulacros que indiquen los pasos y el modo de evacuación ante percances como los mencionados anteriormente?
Nada, una vez me hicieron un examen de la visión de riesgos profesionales.
– ¿Conoce como funciona un extintor? – pues yo tengo uno en mi carro, creo que ha de funcionar lo mismo.

23 ¿Han recibido algún tipo de capacitación acerca de la seguridad informática y su importancia para las organizaciones?
No – ¿o sea lo que se ha podido documentar investigar? – Exactamente – ¿En que aplicaciones ha trabajado en la parte de desarrollo? – Inventarios – ¿De cada uno de ellas cuéntenos en que se la desarrollo? – Informix hay cosa en Visual Basic, la parte de inventarios esta en Informix, Cartera esta en Informix, la parte de las notas antiguas como esta en equipos Windows esta en Visual Basic – ¿tienen licencias? – **NO SE ESCUCHA BIEN**, la otra de fox es la que se toma del aula de informática

Los códigos fuente los conservan? Si aquí están y fox

ANX06

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 2

CARGO: PROGRAMADOR

1. ¿Para la gestión y planeación para el desarrollo de programas en la Universidad de Nariño, quienes son los organismos que determinan el desarrollo de estos programas?
En este momento el comité de sistemas, que es el máximo ente de la universidad encargado de la administración de la tecnología y de los sistemas determinan las políticas y los lineamientos a seguir en cuanto al desarrollo del software de la universidad – ¿Para establecer, ellos, cuales son las necesidades del software se tienen en cuenta las necesidades de la dependencia? – Efectivamente las dependencias tramitan a ellos oficios o solicitudes o proyectos respecto a las necesidades de cada una de las facultades, oficinas administrativas, ellos hacen el correspondiente análisis técnico y determinan la solución que se le comunica a cada oficina – ¿En base a eso, el desarrollo lo realizan ustedes, el personal del Centro de Informática? – El desarrollo de las aplicaciones lo realiza el centro de informática – ¿Quienes revisan esta solicitud directamente? – La solicitud directamente lo puede hacer cualquiera, el Decano, el jefe del centro de informática – ¿Por ejemplo a usted ya le pasan el comunicado de cual es el programa o la aplicación que se va a desarrollar quien le da esa información? – El jefe de la oficina de informática, lo comunica, como miembro del comité de sistemas lo oficializa a nosotros – ¿Se realiza de manera escrita? – De manera escrita ellos hacen una especie de resolución o acuerdo o comunicado en el cual se especifican que o cual es la solución a realizar o cual es el paquete o el software que se debe hacer.

2. ¿En el documento de aprobación se definen de forma clara los objetivos que se tienen sobre el proyecto?

Si el proyecto es aprobado, entonces, obviamente debe haber unos propósitos y unos objetivos que la oficina se persiga respecto al desarrollo del software o la aplicación, entonces cuando ellos aprueban este proyecto pues nosotros nos fijamos respecto al documento y empezamos a hacer el correspondiente análisis en cuestión de tiempos, para las fases que vamos a hacer, entonces colocamos que si se lo puede terminar en dos meses o tres meses, cuatro meses para la realización del proyecto y en el cual nosotros lo vamos a ejecutar – ¿Esa determinación de tiempos, la realizan ustedes o por parte del Comité de Sistemas les establecen a ustedes las restricciones de tiempo y de recursos que tienen? – No, nosotros porque tenemos el conocimiento y la experiencia, podemos decir cuanto tiempo se demora en hacer un software o un paquete y definimos y acordamos con el jefe de la oficina de informática y que lo vamos a realizar en tal periodo de tiempo – ¿En esos periodos de tiempo están incluidos periodos para revisión del software? – pues si, digamos que si es un periodo cíclico – ¿Qué están haciendo revisiones, pruebas? – Con los usuarios – ¿y se establece una fecha de entrega limite? – diríamos que si se coloca en cuanto a meses, si son tres meses, a veces cuatro cundo pueda estar montado el sistema a no ser que haya inconveniente, algo que no se tenga presupuestado

3. ¿Dentro de la planeación del programa, del desarrollo que se va a entrar a trabajar, se especifica algún modelo en especial de desarrollo de software que van a utilizar y las características que van a tener ese modelo que ustedes van aplicar por decir en la planeación determinan trabajar en base al modelo lineal o al modelo en espiral o alguno de los modelos ya establecidos o maneja esto dentro de la planeación, se especifica algún modelo en especial?

Nosotros hemos manejado el modelo cíclico en espiral, nosotros hacemos el análisis, el diseño, programación, pruebas y vuelve a repetirse el ciclo, hasta que quede el software terminado, eso lo hemos hecho siempre porque debido a los requerimientos del sistema o las normatividades o las políticas, ya sea de la universidad, de otros entes del gobierno que controlan digamos las universidades, entonces estamos continuamente en ese proceso cíclico de volver a replantear la aplicaron, analizarla, diseñarla y a programarla y hacerle cambios es un mantenimiento permanente hasta el momento. Existe una política ahorita que pretende cambiar el sistema Financiero de la universidad, el cual se ha propuesto según a directrices del Comité de Sistemas es que sea el modelo Orientado a Objetos, el modelo de Unificado de Modelamiento que se llama UML, el UML que pretende que todo el sistema este enfocado en esa metodología, esta en desarrollo pero en este momento todavía no esta montado la aplicación.

4. ¿Cuando participa un personal externo, llámese pasantes, llámese tesis o colaboradores de alguna dependencia que va a participar en el

desarrollo de ese proyecto, se exige que esas personas tengan un perfil adecuado según las exigencias del proyecto que se va a trabajar?
Si efectivamente en cuanto al desarrollo de pasantías como es el caso las que se están desarrollando existe un acuerdo entre el programa de ingeniería de sistemas con el Comité de Sistemas para definir o escoger a aquellos personajes o estudiantes que van a ser los responsables esos requerimientos, esos requisitos los plantea el jefe de sistemas el cual le define a los directivos del comité de sistemas cuales son los pasantes que características obviamente que deben ser los mejores, los cuales sirven para el desarrollo de ese proyecto

5. ¿Cuando ya se entra a trabajar en la parte del proyecto la documentación que se les entrega a la parte encargada del desarrollo es completa o tiene huecos todavía que hay cosas que no se saben?
Debido a la complejidad del sistema existen cosas que realmente toca ir a averiguar, nosotros hemos entregado la mayor cantidad de documentación que nosotros tenemos del sistema que esta ahorita en funcionamiento, tenemos manuales, reportes, procedimientos que están por escrito, manuales de sistemas de procesos en cuanto a software y aplicaciones, sin embargo existen otras cosas que los maneja realmente el experto en el funcionamiento como contadores, auxiliares de contabilidad, auditores que realmente tocaría irles a preguntar a ellos que particularidades necesitan.
– Si es más o menos completa la información a pesar de que hay cosas que si no están – Toca ir a buscarlas, toca ir a la fuente – ¿y esta información según lo que me dice, esta catalogada o sea la parte de documentación de análisis, la tienen catalogada la información? – Si tenemos documentación de análisis, de diseño, de bases de datos hay de programación, pues de algunos aplicativos si esta completa – Por ejemplo vamos a parte específica nombre del aplicativo y los... – Ah la documentación; el Sistema académico en una parte en el 50% esta documentada, la otra parte parcialmente, tiene análisis, diseño, programación, manuales de operación, de una parte, de la otra, la que inicialmente se monto cuando nosotros llegamos hay manuales pero no esta completa – ¿Quien maneja esa información, digamos nosotros sabemos que en el Centro de Informática, según lo que nos han contado ustedes mismos, cada funcionario maneja como un área, cierto? – Si señor – ¿Entonces es el encargado del área por decirlo de alguna manera quien maneja esa documentación o es el director o es la secretaria o hay una parte donde todos pueden tener acceso? – Si, pues el jefe de la oficina debido a requerimientos que se hacen por ejemplo la Contraloría departamental, pide manuales de procedimientos de sistema, de software, el jefe de la oficina tiene eso y obviamente los demás funcionarios que tenemos a nuestra responsabilidad las aplicaciones pues tenemos el manual del sistema y del funcionamiento de esas aplicaciones y el jefe tiene como director nuestro, toda la documentación.

6. ¿Se cumplen con todos los lineamientos, en este caso usted nos decía que este momento están trabajando en base al modelo en espiral, se cumplen con todos lo lineamientos establecidos dentro de esta metodología?
De acuerdo a las características del modelo, pues hacemos lo que dice el modelo.

7. ¿El proceso de análisis, el proceso de diseño, el proceso de manejo de base de datos obedece a estándares establecidos dentro de los modelos especificados?
Eso es difícil decirlo por que existe el diseño de base de dato por ejemplo, existen modelos de hace quince años, entonces a veces el cambio puede ser riesgoso hay cosas, hay bases de datos, es que las bases de datos no están unificadas son varias base de datos, debido a que esa bases de datos por ejemplo son muy antiguas, entonces cambian la estructura de ellas y seria cambiar todo el software y el sistema completo cosa que acarrearía un tiempo super difícil para por ejemplo cambiarlo de una base de datos pues de un diseño antiguo a un diseño normalizado nuevo porque por ejemplo esas bases de datos que hemos encontrado pues están normalizado hasta la segunda forma normal, entonces nosotros quisiéramos en estos momentos cambiarla a la cuarta forma normal, eso implicaría un cambio super grandísimo y un cambio de todas las aplicaciones entonces, obviamente las aplicaciones nuevas que nosotros hemos construido y nos ha obligado a crear nuevas bases de datos pues las hemos hecho con la metodología que nosotros hemos aprendido o que han aparecido, pero por ejemplo esas aplicaciones viejas no podemos cambiarlas porque acarrearía muchas consecuencias.

8. ¿Cuando se hace el levantamiento de la información se trata de entrar en la mayor profundidad de la investigación para alcanzar todos, todos, y cada uno de los más mínimos requerimientos o se toma un lineamiento general en los requerimientos que tiene los usuarios o el sistema?
La información que de pronto se entregue va a satisfacer la necesidad de urgente, me explico porque a veces por ejemplo la contraloría requiere alguna información, nosotros debemos cumplir con esa necesidad obligatoriamente ya, porque si nosotros nos ponemos a analizar de pronto si optimizamos, pues seria nuestra intención optimizarlo, verdad pero si quisiéramos analizarlo mas profundamente nos corre el tiempo y seria una inconsistencia bastante contraproducente, entonces nosotros tratamos de satisfacer las necesidades pero de lo que se requiere en este momento, ¿porqué?, Porque el tiempo apremia y las cuestiones son urgentes.

9. ¿Cuando se realizan entrevistas en el cargo que se realicen, se detalla o se planifica esa parte donde dice a quien vamos a entrevistar, cuando, hora, fecha y lugar de la entrevista, no se a través de una grabación o a través de un documento que diga listo Srta. Maria Constanza de

contabilidad, quién es el personal encargado, vamos ha hacer una entrevista de tal fecha, a tal hora, a tal lugar y vamos a tratar de esto o simplemente va uno y recoge la información?
Si se concerta con los funcionarios, se concerta con los empleados esos horarios puede haber de pronto un oficio comunicando esas cuestiones un correo electrónico en que se los notifica a ellos para esa cuestión pero previamente se ha hecho un acuerdo.

10. ¿En el proceso de análisis cuando se da la visita o en el momento que se realizan las entrevistas con los usuarios se atiende las necesidades de ellos, necesitamos esta cosa en especial, se atiende ese tipo de necesidades así no sea parte fundamental del proyecto grande, digámoslo de esa manera?
Tratamos de agrupar o si de tomar la mayor cantidad de necesidades de ellos para poderlas satisfacer, siempre va a haber por parte de ellos unas inquietudes y pues en nuestra medida, en la medida de los casos, en el tiempo y en nuestra capacidad tratamos de hacerlo.

11. ¿Pasado un tiempo si los usuarios tienen nuevos requerimientos, esos nuevos requerimientos los hacen por escrito o través de que medios los hacen?
Por escrito, piden por escrito los cambios

12. ¿Se establece algún compromiso por parte de los desarrolladores a establecer esos cambios o esos nuevos requerimientos?
Nosotros recibimos esos requerimientos y los acogemos y pues posteriormente cuando se hace la primera entrega o la entrega de pruebas, corroboramos de que se haya cumplido.
13. ¿El proceso de análisis se encuentra debidamente o estrictamente documentado?
No – ¿Se hace el proceso de análisis pero no se entra a… digamos a transcribirlo? – Transcribirlo no, porque ellos piden es el software

14. ¿Participa personal de auditoria para establecer los controles de seguridad que se deben tener dentro de la aplicación?
Si – ¿Que controles se establecen? – Ellos lo que hacen es una revisión digamos sobre los formatos que se entregan o los reportes, en el caso en estos momentos de matriculas o de contabilidad ellos están periódicamente haciendo revisiones no muy profundas pero si a veces en el funcionamiento del programa por ejemplo en el programa de matriculas que este sacando bien la liquidación, parámetros socio económicos o algunos elementos de reclamos entonces ellos están presentándonos las inquietudes a nosotros o en cierta medida ellos pueden entrar a revisar el software para que se estén entregando los saldos en los balances, si hay una persona sea encargada de esas inquietudes.

15. ¿Dentro de estos módulos de seguridad que se trabaja existe un control de acceso al sistema a través de un nombre de usuario y una contraseña?
Si, para todas las aplicaciones

16. ¿Existe también un registro en el que se identifique el nombre del usuario que ingreso, la fecha, la hora, las aplicaciones a las cuales tuvo acceso?
Si, en algunos aplicativos – ¿Que tanto se registra? –Se registra el usuario, la hora, el dato por ejemplo que se borró o el dato antiguo y el dato nuevo cuando se hace un cambio.

17. ¿Quiénes revisan estos log's o con que periodicidad se realiza esta revisión?
Esa revisión no es periódica se la hace cuando sucede algún problema o alguna inquietud en cuanto a imprecisiones, pero no existe una periodicidad de revisar esto, son grandísimos estos archivos para estar revisando uno por uno, como complejo, cuando hay algún problema que se cambio un dato y que por qué se cambio, por qué se borró entonces uno se remite y les entrego un reporte a los funcionarios diciéndole vea esto paso a tales horas, quien lo hizo y qué cambio.

18. ¿En cuanto a las claves de acceso, existe algún modelo de encriptación para estas claves?
Modelo de encriptación, no eso lo determina el sistema operativo, lo culta– ¿ustedes no tienen un modelo propio en la aplicación? – no, el sistema Unix lo encripta, ahí no se puede.

19. ¿Se establecen niveles de usuario para acceder al sistema, estableciéndoles sus respectivos privilegios?
Digamos que si existe por que a cada usuario le podemos restringir algunas aplicaciones y permitir la entrada a otras, hay por ejemplo usuarios para que consulten pantallas y reportes, hay otros usuarios para que metan datos, actualicen su información y hay otros súper usuarios como nosotros que tenemos aplicaciones en las cuales podemos entrar a todo.

20. ¿En lo que se refiere a la etapa de diseño, ustedes tienen la documentación, en la que se indique la descripción de interfaces, definición a veces de entidades cuando se refiera al modelo…?
Esta hecha parcialmente, no esta total

21. ¿Se garantiza que los datos eliminados por los usuarios se guarden temporalmente en otros archivos?
Si están en otra tabla, no se borran – ¿Cuanto tiempo permanecen ahí? – Permanentemente, todo el tiempo, siempre que estemos ahí, ahí van a estar.

22. ¿Para dar aceptación al diseño de un aplicativo se cuenta con la aprobación de los usuarios?
Si ellos como son las personas encargados de seguir utilizando el programa, ellos son los que dan el visto bueno o el cambio que se le debe hacer.

23. ¿Mientras realizan el desarrollo del programa están estableciendo reuniones con el director del centro de informática y los usuarios que vayan dando su concepto de aprobación?
No, eso se hace separado, por que de pronto el director de la oficina nos hace los requerimientos entonces nos reunimos nosotros para evaluar todo eso y diríamos que es de nosotros estar con los usuario, conversaríamos, existen a veces reuniones extraordinarias pero no se dan periódicamente, en los cuales se ha convocado a todos, la mayoría de los funcionarios para analizar junto con el director de la Oficina de Informática o el vicerrector o los encargados del comité para analizar el software, de una manera general específicamente, no se ha hecho.

24. ¿En la parte de programación digamos en el código, las fuentes, se encuentra documentado de manera que se especifique cuales son las rutinas, que tipos de variables se están utilizando, eso se documenta internamente dentro del código como comentarios?
Si se ponen comentarios, estos son los procesos, esta rutina es de tal procedimiento o esto sirve para hacer tal estado, tal reporte, en el encabezado de cada programa esta la función principal del programa y después en las funciones o en los procedimientos, se escribe para que sirve cada función, que variables de entrada tiene, pero realmente es muy largo para uno acordarse.

25. ¿Los programas poseen internamente sus propios procedimientos, que permitan recuperar información en el caso de un fallo por ejemplo del sistema, digamos sabemos por ejemplo hay ciertos programas que en el momento que haya una caída de luz, se borran, se pierden las relaciones, cierto hay algún proceso interno de los programas que permita recuperar o hacer restauración de archivo?
Tenemos rutinas en cuanto en la base de datos que reparan las tablas o que reconstruyen los índices o que sacan copias en archivos planos en el caso de esta base de datos, es recursivo todo – ¿Me imagino que manejen controles, para identificar y corregir los datos? – Si

26. ¿Se mantienen copias de seguridad de los programas fuente, durante el desarrollo?
Si yo tengo tres, la tengo en mi computador, en el servidor, en mi casa, tengo en todas partes.

27. ¿Se encuentran definidos algunos estándares para la programación?

Estándares....estructurada, nos basamos en la programación estructurada en este momento, hay otras aplicaciones en Windows que están orientadas a objetos.

28. ¿Internamente en el centro de informática tienen establecida alguna política para la programación?
Pues realmente eso es subjetivo, aunque todos hablamos el mismo idioma, en la cuestión de las aplicaciones son estructuradas, las aplicaciones en Windows son orientadas a objetos y la otra la nueva que también es orientada a objetos.
29. ¿Digamos en este sentido el centro de informática determina que las variables por ejemplo lleven un tipo especial de nombramiento, que las funciones lleven un tipo especial de nombramiento para que todo este unificado en todos los programas?
Para evitar la confusión entre los diferentes programas, pues cada uno tiene sus aplicaciones en su sistema, pues hay varios sistemas dentro del sistema general entonces hay unas iniciales unas marcas que determinan quien fue el que hizo el programa y obviamente puede la una persona interactuar en el otro pero sin lugar a que de pronto haya una rutina de validación y que todos van a hacer la misma toca colocarle algo para diferenciarla no le puede borrar el un programa al otro.

30. ¿El modulo de seguridad que se especifica en el diseño es coincidente con el desarrollo, en la parte con el desarrollo que ya se realiza?
Si, eso se debe hacer, de acuerdo a las políticas y experiencias que nosotros tenemos es un requisito indispensable porque ya conocemos a veces los problemas que se pueden dar con los funcionarios de pronto por error o por confusión pueden alterar algún dato toca saber que paso y en la mayoría de los programas se hace eso.

31. ¿Los usuarios de los diferentes programas entran al sistema a través de un login y un password?
Si – ¿se evita la visibilidad de la contraseña? – Si – ¿se valida la utilización de caracteres especiales en la contraseña? – Lo define el sistema operativo – ¿o sea la parte de contraseñas es todo en base al sistema de logeo de Unix? – Si – ¿Ustedes no manejan ningún tipo de aplicación respecto al acceso, un sistema de logeo propio? – En algunos programas, si existe, se acoge – ¿se realiza un cambio periódico de las contraseñas a los usuarios? – periódico no – ¿es por requerimiento del usuario? – Si, correcto – ¿los usuarios pueden hacer cambio de determinado…? – No.

32. ¿Existe un registro de fecha, hora y cambio de las contraseñas?
No, de pronto en el sistema debe estar

33. ¿Las personas que realizan las pruebas de verificación son distintas a las que desarrollan el sistema?
La misma persona que hace el software, hace las pruebas y puede hacer pruebas con los usuarios finales o puede hacer prueba el señor de auditoria que puede llegar a revisar el programa – ¿Pero en ningún momento lo ha hecho el auditor? – ¿El auditor? – ¿ha estado en las pruebas? – no, cuando él tiene la inquietud va y dice revisemos y revisamos.

34. ¿Los resultados de las pruebas se documentan, por ejemplo aparece un error, se documenta o apareció error en tal parte o se entra a corregir automáticamente?
Nosotros tenemos unas notas, pero son notas individuales de cada funcionario, de cada programador apunta los problemas que encontró y posteriormente procede a corregirlos.

35. ¿se utilizan datos de prueba o se entra a hacer pruebas en tiempo real con datos reales o sea ya en el momento de poner a funcionar?
Con datos de prueba y después con datos reales – ¿o sea una vez se apruebe el sistema? – una vez montado el sistema.

37. ¿los archivos de prueba o los datos de prueba se identifican plenamente, o sea ustedes tienen establecidos unos datos que les sirven para prueba o simplemente toman en ese momento unos datos?
De acuerdo a los condicionantes del software o los aplicativos escogemos algunos modelos, cogemos del universo de los que nos sirven, los que se acogen a esas condiciones son para probar, para tomar todas las condiciones que tenga el programa desacuerdo a tal condicionamiento al cual debemos corroborar el resultado final.

38. ¿Estos datos de prueba una vez esta corriendo o si las pruebas se hacen sobre la marcha en el momento de extraer la información, se hacen bajo autorización o se eliminan directamente?
Digamos que si, esos se quitan para evitar problemas con los datos reales.

39. ¿Se realizan pruebas de escritorio?
A veces si, cuando la complejidad lo requiere toca – ¿Esas se realizan bajo autorización o…? – cada programador la hace, es autónomo.

40. ¿Las pruebas de aceptación quien las realiza el programador o los usuarios, del funcionamiento ok del programa?
Los usuarios finales dan el visto bueno – ¿Cuándo se hacen las pruebas, se establecen documentos por escrito, por grabación o por algún otro documento en donde se explique, se especifique fecha y hora de la prueba? – Esa circunstancia no, de pronto hay unos oficios de recibido respecto al software que se entrega, que esta en funcionamiento y que de pronto el funcionario

puede firmar como recibido o aceptado. – ¿Hay se especifican lo procesos que se realizan, las pruebas? – si, diríamos que sí – ¿y en general los programas también? – incluidos los programas, en qué módulos – ¿se documenta también en que equipo se utilizó, se realizan las pruebas? – Si el equipo también.

41. ¿Los usuarios y el director del centro firman un documento en que se apruebe a conformidad las pruebas de aceptación?
En algunos casos si, en el que se presente algún problema que requiera responsabilidad, se hace un oficio en el cual la persona firma de recibido y ha aceptado la modificación que se haga realmente la circunstancia lo amerita.
42. ¿Quién realiza la capacitación de los programas?
Los programadores – ¿cada programador que desarrollo su modulo? – Lo capacita al funcionario para que lo maneje, lo manipule – ¿existe alguna planeación para dictar esta capacitaciones? – de pronto el programador de acuerdo como ha diseñado el programa hace un bosquejo de lo que le va a indicar al funcionario para que le quede mas fácil aprender el programa – ¿la capacitación se hace en una sola sesión, en dos, tres, varias sesiones? – se hace, se programa regularmente, diario o pasando un día para que sea periódico el aprendizaje del mismo porque no podemos hacerlo en una sola sesión. – ¿los usuarios reciben la capacitación absoluta del programa o sea todo lo que ellos necesitan y un poco mas o es restringida a esto específicamente es así, así y así o se amplia un poco mas la parte de la capacitación, por ejemplo con un usuario nuevo, tomemos el caso de una persona que recién se vincula a la Universidad y que va a entrar a trabajar en base a un sistema y el caso de una persona que ya viene trabajando algunos años y se le monta un sistema para ellos? – Es pertinente explicarle todo y si el tiene alguna duda o alguna inquietud es pertinente acogerlo para explicarle o reafirmarle lo que se haya dicho si hay alguna duda.

43. ¿A los usuarios se les entrega documentación, frente al programa, manuales de usuario, manuales de procedimiento, bosquejos o unas hojas en donde se llega a los procesos?
Ellos toman nota de esos procesos – ¿pero no existe un manual? – No.

ANX07

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 3

CARGO: *PROGRAMADOR*

1. Existe un inventario del software del Centro de Informática?
Hay una relación de los programas, que se ha entregado a Contraloría Departamental, nos han solicitado qué programas existen, de todos los módulos que hemos hecho, se reposa un listado de todo lo que hemos hecho.
- ¿Este se encuentra en el Centro de Informática? El jefe lo tiene
- ¿Frente a software, aplicativos como Sistema Operativo, Antivirus se tiene un control de los programas adicionales a los que desarrollan de los que se encuentran instalados? Dentro de los requerimientos que hizo la Contraloría nosotros relacionamos, estaba en ese informe, todo tipo de programas y Sistemas Operativos. – ¿El Inventario que corresponde al Sistema Operativo y los programas es el mismo que tiene almacén? El comprado si

2. ¿En lo que se refiere a Licencias todo el software que se encuentra en el Centro de Informática cuenta con licencias?

No, algunos son gratuitos bajados de Internet, la licencia de Unix es de Corponariño fue tomada de allá, _¿Cómo se hizo el convenio? No, no lo conozco.

– ¿Las aplicaciones que están en Visual Basic y Fox? Esas se acogen a la licencia Campiu que tienen la Universidad con Microsoft, todas las aplicaciones que se desarrollen, se acogen a esa licencia.

-¿Es un tipo de licencia corporativa, educativa? esa es educativa - ¿Pero permite hacer desarrollos para uso de la Universidad? Correcto.

3. ¿Para la adquisición de software se consideran todas las necesidades que tiene la institución?

Si, el estudio lo hace el comité de sistemas de acuerdo a las necesidades que hagan las diferentes dependencias o las oficinas, de que software, licencias o aplicaciones que se necesitan para poderlas adquirir.

- Últimamente, esta el caso del software que se adquirió de Pamplona cierto, entonces cuando se adquirió este software, se revisa que contenga el módulo de auditoría?- La exigencia del módulo de auditoría no ha sido una prioridad hasta el momento, el módulo académico, lo que ha preocupado a la universidad es que tenga las mismas funcionalidades del que manejamos ahorita en el sistema Unís esa es la preocupación mas reciente de los administrativos, en este momento se esta haciendo el estudio para mirar si tiene o no tiene las mismas funcionalidades o las aplicaciones que nosotros manejamos, o sea estamos en proceso de verificación. – ¿Pero si manejan módulo de Auditoría? Ellos nos dijeron que tenia Auditria a todos los registros que se realizaban, sin embargo todavía no lo hemos constatado físicamente, no sabemos pero ellos dicen que existen.

-¿Este software permite tener control de acceso de usuarios? –Si, ellos lo tienen. ¿Cómo lo realizan? – Contraseñas, Login, fechas y horas de ingreso, tipo de operaciones que se realicen en el aplicativo. – ¿Permite realizar el software backups? – Supuestamente si, aun no lo hemos hecho las pruebas.

Independientemente, no hablemos de la adquisición del software de Pamplona, en general para la adquisición de software, si se establece como requisito, la cuestión de Auditoría, Control de Acceso, Backups? –Correcto, es una prioridad.

4. Seguimos con lo que es la adquisición de Software, ¿Cuando se adquiere software se valora el hardware existente en la Universidad?

Correcto si se hace un estudio de acuerdo a los equipos o a los computadores, que se tiene para poder ser instalado en los equipos.

5. Ahora hablemos de antivirus, ¿Ustedes tienen instalados antivirus en los computadores del Centro de Informática?

Si, están instalados antivirus -¿Qué antivirus tienen instalados? Esta uno que se llama Antivir, Norton, habían Viruscan.

6. ¿Se esta actualizando los antivirus?

Si, por Internet se actualizan. – ¿Ustedes están pendientes de las actualizaciones que hacen los proveedores? –Si -¿Mas o menos en que periodo realizan este procedimiento? – Cada tres meses puede ser.

-Manejan algún software que realice control de gusanos, espías o troyanos? – Spydoctor - ¿Se actualiza en lo que se refiere a Parches y otras actualizaciones para el Sistema Operativo? – También, se bajan de Internet las actualizaciones. ¿Quién se encarga de realizarlas directamente las actualizaciones? Freddy – El es el directo encargado? –Si.

7. Existe alguna política que antes de ser leído un medio externo, como disquete u otros discos, deben vacunarse?

Si, claro. –Siempre realizan este proceso? – se acoge a la norma que tiene el Aula de informática. -¿Cuál es la norma? –hay una especie de circular en que el Aula de Informática le pide a las oficinas que deben revisar los archivos, en los computadores de cada funcionario.

8. Como ultima pregunta en este aspecto, ¿Los antivirus cuentan con la respectiva licencia?

Los antivirus son bajados de Internet. –En caso de Norton ... Norton 30 días? – Norton el Aula de Informática tiene, algunos si están amparados por el Aula de Informática, otros son gratuitos.

8. Hablando de bases de datos, ¿en el diseño de bases de datos que ustedes realizan en el Centro de Informática, se contemplan tablas para el control de usuarios?

Si, hay tablas de Auditoría - ¿En estas tablas se especifica los privilegios de los usuarios frente al sistema que van a trabajar? –No, –¿Registran las actividades que realizan los usuarios? SI, -¿Qué campos contemplan estas tablas? Usuario, hora, la tabla que ha sido modificada, que tipo de operación se ha realizado sea adición, modificado o eliminado, dato anterior y dato nuevo.¿todas las aplicaciones manejan este control?- La mayor parte.

9. ¿La información que ustedes alojan en los bancos de datos se encuentran encriptadas?

Encriptadas no. –¿Y cuando se hace la parte de ingreso ? -Las claves cuando ingresan, si aparecen encriptadas -¿Con mecanismos de encripción del Sistema Operativo?-Del Sistema Operativo.

10. ¿El control de usuarios que Ustedes lo realizan lo hacen directamente por Sistema Operativo y Aplicación o solo por Sistema Operativo o solo por aplicación?

Por ambas, Sistema Operativo y Aplicación, o sea se loguea el Sistema Operativo y nuevamente se hace control sobre el usuario.

11. Sabemos que realizan backups, ¿Existe un documento en que especifique procedimientos, como fecha, hora?

No, es responsabilidad individual. -¿Cada cuánto hacen backups? –Diarios. ¿De todos los sistemas? –De todos los sistemas a medio día y a las seis de la tarde.

12. ¿Han tenido caída de algún sistema, en que hayan tenido la necesidad de restaurar la Base de Datos?

Si, problemas de electricidad, cortos circuitos, se fue la base de datos y toca recuperar todo. -¿Existe un procedimiento por escrito que indique los pasos a realizar en una falla de estas? –No, no esta establecido. -¿Pero si están preparados cuando se presenta esto, tienen un Plan de Contingencia? –Si hay equipos de apoyo, computadores de apoyo y múltiples copias que nos permiten restablecer el sistema a su normalidad.

13. Frente a la parte eléctrica, ¿Usted tiene conocimiento si se desarrolla algún mantenimiento a las redes eléctricas del Centro de Informática?

–Mantenimiento... -¿Hay personal especializado que este pendiente de los circuitos eléctricos, de toma corrientes, medidas de voltaje, del cableado? –Ha habido hasta el momento una serie de problemas en el flujo eléctrico que han obligado a la revisión en los últimos seis o siete meses. –Pero a nivel correctivo. -¿Qué problemas han tenido? –Picos de corriente alta, que han ocasionado problemas en el sistema. -¿Las personas encargadas son de servicios generales? –Son contrataciones externas a ingenieros eléctricos que se encargan de revisar.

14. ¿Usted cómo puede catalogar la respuesta frente a un daño eléctrico por parte de los contratistas, es inmediata, se demoran?

No, si es adecuada la respuesta, si es en un tiempo prudencial, rápida.

-¿Estos contratistas realizan mantenimiento preventivo? –No, No hacen.

15. ¿EL Cetro de Informática cuenta con sistema de respaldo eléctrico, UPS?

Si hay UPS. -¿Cuántas UPS tienen? –Hay dos, son nuevas, una para el Centro de Informática y otra para Contabilidad. -¿Las dependencias cuentan con UPS? –No. -¿OCARA? –OCARA con una UPS de capacidad baja, Almacén con una UPS que deja solo para quince minutos. -¿Cuál es la Capacidad de la UPS del Centro de Informática? –Tres o cuatro horas.

16. ¿Tiene un sistema de respaldo en el sentido de Planta Eléctrica?
No, no hay planta eléctrica de respaldo. ¿La Planta que tienen la Universidad en la parte de abajo? –Esta dañada, esta de adorno, creo que era solo para el Centro Administrativo que antes funcionaba allá, en el tiempo que yo estoy no la he visto funcionar.

17. En el momento en que se genera una caída de energía, ¿Cuáles son las actividades que realizan en los sistemas que no tienen batería de larga duración, hay una persona que se encargue de cerrar los sistemas?

Cuando se va la energía, el Centro de Informática tiene un circuito aparte, circuito eléctrico privado digamos, entonces se puede ir la energía en las demás oficinas pero en el Centro de informática sigue con la señal de los servidores, entonces no hay problema, pues la gente conoce el hecho que se fue el fluido eléctrico y hasta ahí llegamos, sin embargo los datos la información quedan en los servidores del Centro de Informática. -¿El suministro de Energía del circuito eléctrico del Centro de Informática, quién lo hace? –Ese esta dependiendo de la UPS nuestra. -¿y por ejemplo en almacén, ellos manejan propio servidor, entonces alguien va a..? –Ellos mismos lo realizan, cuando se va la energía, la UPS tiene hasta quince minutos y apaga el servidor, la persona que maneja inventarios se encarga, tiene manejo del servidor ahí.

18. ¿El mantenimiento a las redes de datos quién lo realiza?¿Preventivo?

Lo hacen los funcionarios del Aula de Informática, ellos tienen el control de la red de datos. -¿Lo hacen periódicamente? -cada vez hay un daño, es correctivo. -

¿En el Centro de informática existe un registro de los mantenimientos practicados? –No, yo no he visto registros escritos.

19. ¿Los sistemas Operativos que manejan, tienen alguna configuración especial, frente a controles de acceso, tienen habilitados los sistemas de logs?

Si hacen una serie de configuraciones -¿Qué Sistemas Operativos Manejan? – Unix Open Server 5.0, hay Linux, Windows XP.

20. ¿Tienen configuraciones para el manejo de contraseñas que le exija al usuario un mínimo de caracteres?

Esa verificación de las claves las hace el administrador de la Base de Datos. -¿Las claves las asigna el mismo usuario, o son asignadas por el sistemas o digamos por el Centro de Informática? –Las escoge cada usuario pero tiene que ser validada por el administrador del Sistema. -¿El administrador las conoce? –Hay dos tipos de clave, usuarios del Sistema Operativo estan encriptadas, y las otras si.

ANX08

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 4

CARGO: *PROGRAMADOR*

1. ¿Existe el Diseño de la red de datos?
La empresa que fue contratada para hacer el diseño de la red dejo únicamente, el cableado que hay entre el tablero y los puntos, los puntos no fueron numerados correctamente, razón por la cual debido a que de todas formas tocaba hacer la instalación de los computadores nosotros reasignamos el numero de los puntos, en el momento entonces las cajas de las oficinas tienen su numero correspondiente con el panel central.

2. ¿Actualmente existe un documento en que se especifique la numeración y ubicación correspondiente de cada punto de las dependencias?

No, no la hemos elaborado simplemente se hace visualmente, en el momento de hacer algún mantenimiento.

3. ¿Se realiza mantenimiento a la red de datos?
No, solamente cuando los usuarios digamos no tienen ninguna conexión, entonces en ese momento se hace la revisión para ver si fue el pathcord, tiene el daño, o el punto que va entre el cableado central y el punto correspondiente.

4. ¿Quiénes realizan el mantenimiento?

De aquí algún funcionario del Centro de Informática.

5. ¿Qué control se maneja para el acceso de usuarios a las aplicaciones?

Como el sistema operativo del Centro es Unix, entonces los diferentes usuarios tienen acceso en las oficinas administrativas que son Contabilidad, Presupuesto, Tesorería, entonces tienen una clave que se hace por aplicativo, es decir hay una para Contabilidad, otra para Presupuesto, otra para Tesorería y Recursos Humanos después del primer acceso adicionalmente cada usuario tiene una clave adicional, que es una clave propia de cada usuario, generalmente viene con su nombre y una clave que ellos mismos han escogido cuando se crea dicho usuario. Las claves entonces, las claves de Contabilidad y presupuesto, entonces no se las cambia nunca pero si la de los usuarios, en caso que el usuario cambie, entonces el usuario es retirado del sistema y quedan vigentes únicamente las personas que tienen derecho. - ¿Para acceder al sistema maneja contraseña del Sistema Operativo y luego contraseña del aplicativo? - Si, correcto.

7. ¿Qué especificaciones se tienen para que los usuarios escojan su contraseña?

Nada ellos simplemente se les da acceso a un programa, y ellos la cambian a su gusto, que pueden utilizar numérica o alfanumérica, eso básicamente hasta un máximo de diez dígitos.

8. Me comenta que no realizan cambio de contraseña, entonces, ¿Bajo qué parámetros se realizan cambios de contraseña?

No, únicamente cuando el usuario detecta que alguna persona estuvo a su lado y de pronto logro observar su contraseña, y algunos usuarios que tienen mejores hábitos, ellos hacen que cambie de contraseña mas o menos una vez por mes.

-¿Pero el Procedimiento digamos ellos no lo hacen directamente, sino que hacen la solicitud al Centro de Informática? – Si correcto.

10. ¿El sistema maneja que se registre, cuando se realicen cambios de contraseña?

Sí, en la tabla de auditoria donde se va haciendo ese almacenamiento, cada contraseña dice la fecha y la hora en que fue modificada. –Al igual que todos los procedimientos. ¿Cada cuanto se revisan estos Logs? – Eventualmente si alguien pidiera una auditoría, pero no se hace una revisión.

11. ¿Con qué frecuencia se realizan procedimientos de backups?

Bueno los backups se realizan todos los días, entonces están programados automáticamente los equipos los disponen tres servidores en este momento disponen de una unidad tape backup con capacidad de ocho gigas, en cintas que se llaman minicard, entonces cada uno lo tenemos programado para que mas o menos a las diez de la noche automáticamente haga copia de seguridad, dichas cintas al otro día son cambiadas por otras cintas, entonces tenemos en total ocho cintas, las cuales las vamos turnando, entonces una comienza el lunes, otra el martes hasta que el ciclo vaya cambiando. -¿Todos los sistemas manejan este procedimiento de backups? Sí, los tres sistemas están utilizando este sistema.

12. ¿En dónde se almacenan estas copias de respaldo?

Las copias de respaldo las almacenamos dentro de la oficina, y periódicamente llevamos a otro sitio las cintas, las copias de seguridad, como por seguridad en caso que hubiera algun siniestro en la universidad o alguna toma de estudiantes.
-¿En dónde se tienen estas copias? – bueno algunas las lleva el director de la oficina. -Hay una copia fuera de la Universidad, otra aquí en la oficina. ¿Existe una copia dentro de la Universidad que no sea el Centro de Informática? – No.

13. ¿Cómo se controla el acceso a estas copias?

Bueno simplemente las copias, la persona que este encargada de las copias de seguridad, es quien tiene en su escritorio normalmente, son de fácil acceso realmente. -¿No existe un sitio adecuado para el almacenamiento de cintas? –No, no existe un sitio adecuado.

14. ¿Existe algún procedimiento escrito para la restauración de backups?

No, pero la copia como es total del disco duro, entonces es de conocimiento aquí de todos los funcionarios, de que en caso de daño del disco duro, se debe bajar el ciento por ciento de la copia de seguridad, restaurando así el día inmediatamente anterior en su totalidad.

15. ¿La información de las backups se encuentra encriptada?

No, no se encuentra encriptada.

16. En lo que se refiere a mantenimiento de equipos, ¿Cada cuanto se realiza mantenimiento?

Aproximadamente cada dos meses, entonces hacemos mantenimiento preventivo básicamente en quitar un poquito de estática a los computadores, quitarles un poco de polvo, pero realmente como los sistemas permanecen prendidos toda la semana, es difícil apagar el sistema y realizar su mantenimiento, y prácticamente los mantenimientos son de...los discos duros son Scossi son de buena calidad realmente son discos duros que están elaborados para trabajar todos los días del año, sin ningún problema, muchas veces el mantenimiento resulta contraproducente porque en lugar de hacerle un beneficio al equipo, puede dañarle la información, mas bien evitamos un poco tocar los servidores.

17. ¿Quiénes se encargan de realizar el mantenimiento?

El mantenimiento de los equipos lo hago Yo, para todos los equipos del Centro de Informática. -¿Mantenimiento digamos tanto de la parte de hardware como se software? – Si en este momento Yo me encargado de la administración del Centro, Yo me encargo que funcionen impresoras, cualquier tipo de dispositivos, terminales remotas, conectividad.

18. ¿Cuentan con un sitio adecuado para el mantenimiento y con las herramientas adecuadas para realizar esta actividad?

No, algunas herramientas como el ventilador cuando se quita el polvo, no lo presta otra oficina, la oficina de Contabilidad y equipo para el rsto solo se necesita un destornillador de estrella para ajustar o aflojar algunas tarjetas de control, tenemos

la ponchadora, no tenemos un probador para los puntos de red, eso no lo suministra el Aula de Informática.

19. ¿Se realiza mantenimiento a la red eléctrica?

Si generalmente estamos haciendo revisiones, casi se podría decir que no es de carácter preventivo, en la Universidad generalmente es cuando ya han ocurrido sucesos de choques eléctricos y demás, es que se ha hecho los controles, claro que lo único que hacemos aquí es revisar la UPS, que este suministrando el voltaje adecuado . - ¿Existe un encargado que revise? No, en la oficina tenemos un tester hacemos revisión de ves en cuando, también tenemos una bitácora por fechas uno va haciendo anotaciones. -¿Lo realizan Ustedes? –Si lo realizamos aquí en el Centro de Informática.

20. ¿Cuándo se presenta un daño, a quién lo reportan?

Pues normalmente cuando son eléctricos a servicios generales, cuando el daño es por consecución de repuestos, se solicita al comité de sistemas solicitando el elemento que se ha dañado, en caso de memoria, disco duro o cualquier elemento de control del equipo.

21. ¿Cuentan con planta de respaldo eléctrico?

No, simplemente la oficina, tiene una UPS con capacidad de 2000.

22. ¿Cuando se hace instalación del Sistema Operativo se realiza con autorización?

No pero realmente la ultima instalación se hizo hace cinco años.

23. ¿Para la escogencia de Sistema Operativo que requerimientos tienen en cuenta ustedes?

Pues realmente el numero de usuarios concurrentes, la velocidad del Sistema Operativo, en nuestro caso, el software que venimos trabajando mas o menos una versión desde 1985 no ha sido actualizada, así que los requerimientos del Unix realmente no se han cambiado.

24. ¿Se encuentran instaladas las herramientas de seguridad propias del Sistema?

Si el Unix posee lo que es Kerbeos 5.0, que le da todo el sistema de control, y adicionalmente de Internet hemos bajado algunos parches de seguridad producidas por la misma compañía de S.O, Santacruz Operation, que es la que nos garantiza que el Sistema funcione correctamente.

25. ¿El Sistema Operativo cuenta con la licencia correspondiente de uso?

La licencia que tiene en el momento, es una licencia para cinco usuarios.

26. ¿Ustedes los funcionaros del Centro de Informática conocen el Sistema Operativo en lo que se refiere a instalación, configuración y funcionamiento?

Creo que sólo Yo tengo el mayor conocimiento por experiencia, por antigüedad, todos están n capacidad de manipulación pero de lo que estado en el Centro Yo me he encargado de la instalación y el mantenimiento.

27. ¿El Sistema Operativo tiene mecanismos de recuperación, para restablecer el sistema en caso que este se caiga?

Si simplemente tenemos una imagen de lo que es ell Sistema Operativo, que esta en cinta, para recuperarlo en lapso de unas dos horas y lo que es bajar la información nuevamente en unas tres horas, de todas formas la Beos con el disco duro tienen un sistema que le avisan con anticipación de un daño, si se van dañando discos Unix lo que hace es copiar esa información en sectores buenos, cuando llega a un limite, el suministra información que el disco duro puede dañarse, cuando es muy grave tocaría volver a bajar la información.

28. ¿El Sistema Operativo esta incluido dentro de los recursos de respaldo, fuera del sitio?

No, hasta el momento no.

29. ¿Han realizado cambios de fecha en el Sistema Operativo?

Si, solamente se hizo cambio de fecha, cuando hubo cambio de milenio y se bajo el parche correspondiente, porque se descuadraba.

30. ¿Se protege el sistema, realizando pruebas, en un servidor de pruebas?

No se utiliza el mismo equipo pero en otro directorio cuando uno ve que la versión es correcta, entonces remplaza la versión si es de cambio, o si el programa es nuevo simplemente se la coloca en el menú para que los usuarios tengan acceso a el.

31. ¿Existe control de permisos a los usuarios sobre los archivos?

Si, cuando creamos los usuarios de programas, entonces en algunos módulos tenemos opciones de que puedan solo ellos hacer consulta, puede ser el Vicerrector, el Tesorero o el jefe de Contabilidad, ellos solo pueden observar la información pero no pueden modificarla, únicamente los auxiliares que estén a cargo de la información pueden modificarla.

ANX09

ENTREVISTA CON EL PERSONAL DE INTERNET

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **WEB MASTER**

1. ¿Qué servicios de Internet presta la Universidad de Nariño?
Servicios de Internet como tal están correo electrónico, transferencia de archivos, publicación de paginas web lo que es http, básicamente esos si, los otros sobre consulta de notas son aplicaciones que se han desarrollado para Web entre esas tenemos consulta de notas, sistema de matriculas por Internet, tenemos el sistema de registro de calificaciones por Internet, un sistema de consulta de hoja de vida que solo lo pueden utilizar los administrativos, sistema de estadística ICFES para uso de OCARA ese sistema saca reportes de que estudiantes están por encima o por debajo de ciertos niveles, estadísticas completas, básicamente eso es lo que tenemos y tenemos también el servicio conmutado es decir permitimos a los profesores y a los funcionarios conectarse a Internet desde su casa por línea telefónica

2. ¿Qué lenguajes utilizan para estas aplicaciones?
Para desarrollo utilizamos, Php, utilizamos Pert, el lenguaje C, utilizamos en ciertas partes ASP y el lenguaje para las bases de datos que es SQL como motor de las bases de datos utilizamos Postgress y Mysql, y como herramientas de diseño están Dream Weaver, esta flash, esas aplicaciones.

3. ¿Qué tipo de servidores utilizan?
Tenemos, en total siete servidores tres de ellos trabajan con Sistema Operativo Linux Son maquinas basadas en arquitectura X86, es decir clones común y corrientes sino que tiene mas memoria y un buen procesador, esas máquinas son Linux, tenemos tres servidores que tienen Solarix, esas máquinas son de arquitectura Spack una arquitectura propia de SUN y trabajan con sistema operativo Solarix que es propio para esta máquinas, Solarix 9.0 y Solarix 8.0 tenemos instalados en esas máquinas y una la que falta es un clon en el que funciona Windows 2000 Server funciona para las aplicaciones que necesiten Windows, las páginas en ASP aquí se publican las paginas web que hacen

muchos estudiantes como tesis, ellos tiene libertad de hacerlo en lo que quieran el todo es proveerles la plataforma, muchos la hacen para Windows.

4. ¿Los servidores están dedicados para un solo propósito o lo comparten?
Están dedicados para propósitos particulares, uno es solo proxy, otro administra correo electrónico de estudiantes, el otro administra una base de datos y otro las aplicaciones web, si están designados para estos servidores, pero de todas formas casi todas tienen lo mismo, pero están detenidos, están en Stanbay, si falta la máquina levantamos los servicios de las otras, lo que paso en este momento se cayó un proxy fue daño físico de la máquina entonces levantamos la otra no más y se va a revisar que paso con eso es un sistema de respaldo que hay allí.

5. ¿Quién es el proveedor de Internet?
Telecom.

6. ¿Qué servicios de seguridad les ofrecen ellos para Internet?
Ninguno el proveedor nos entrega un canal limpio de datos a Internet, la seguridad y la protección esta a cargo del cliente.

7. ¿Qué responsabilidad tiene Usted de la información que se publica o sobre las aplicaciones para Internet?
La responsabilidad que tengo... – ¿Es el directo responsable? – Si...ahí depende del proceso por ejemplo en el proceso de registro de calificaciones, soy responsable que esa información sea consistente, que se pueda garantizar, pues que se pueda confiar en ella porque esa información se genera totalmente desde el sistema, pero hay otra información por ejemplo matriculas que mi sistema depende de la información de OCARA, entonces los responsables en este caso son de OCARA, Yo los proceso y les entrego la información, esa información que les entrego si es mi responsabilidad, ya estudiantes matriculados, materias matriculados es responsabilidad mía, pero por ejemplo si allá me dicen que este estudiante puede ver cálculo, yo le hago ver cálculo y el estudiante como tal no tenía que ver cálculo entonces es responsabilidad de allá.

8. ¿En cuanto a las aplicaciones que se desarrollan para Internet, qué medidas de seguridad se exigen a los desarrolladores que implemente en el programa?
Se les exige haber, primero se recibe las aplicaciones sí, realmente exigirles así como unos estándares no hay, pero se los recibe, nosotros les hacemos una serie de pruebas, revisamos pedazos de código – ¿Exactamente qué les revisa? – Sobre todo la parte de autenticación y acceso a ciertas áreas, digamos privadas del sistema, el sistema tiene áreas publicas y privadas, entonces el acceso a esas áreas privadas, tenemos la autenticación como seguridad, en casos donde es necesario utilizar métodos de encripción hay que hacerlo por ejemplo en el sistema de calificaciones hay que hacerlo por ejemplo en el sistema de calificaciones hay que utilizar encripción, hay que utilizar una especie de firma

digital. – ¿Se revisa el código de tal manera para verificar que no hayan Caballos de Troya o bombas lógicas? – No, no esa es una de nuestras debilidades. – ¿Básicamente por tiempo, o por qué razón no lo realizan? por tiempo lo que pasa es que hay muchas actividades que realizar acá, y hay muy pocas personas, entonces acá hay que hacer..., hay organizaciones en que hay una persona que se dedica exclusivamente a los servidores, otro a las aplicaciones, otro a la red, y acá solo habemos dos, entonces, es como complicado, no se puede por tiempo y realmente confiamos en la buena fe de los desarrolladores, pero perfectamente nos podrían hacer meternos un Caballo de Troya, uno de esos programas que uno no sabe, de las aplicaciones que le he mencionado en la que soy responsable sí, pero de las otras...también es responsabilidad mía, pero es difícil probar eso.

9. ¿Describa como están conectadas las dependencias, básicamente de OCARA, Almacén, Contabilidad, Recursos Humanos y Tesorería con el Centro de Informática en la gestión física de la Red?

A ver nosotros tenemos dos redes la primera cubre digámosle así: lo que es el centro de Informática, OCARA, trabaja Almacén, Tesorería, Contabilidad, esas son las oficinas mas grandes que conforman esa red, hay otra red, que es la que llamamos de Internet que esta conectado el resto de la Universidad -- ¿Todo? -- Si están las aulas, las oficinas, toda la universidad esta conectada a la red y hay otra red, tres tenemos, que es la de servidores, esta red de servidores es la que se conecta a Internet, nosotros tenemos que prestar servicios de Internet y la red de servidores aquí esta nuestro primer firewall y acá tenemos otro, que nos conecta acá -- ¿Estos firewall son filtros? – Si -- ¿Básicamente sobre que están controlando, el acceso? – Estos firewalls, controlan solo el trafico que nosotros queremos permitir, por ejemplo cerramos los puertos de telnet de acuerdo a los reportes se ve la vulnerabilidad del protocolo find algunos de rlogin, se los cierra, este firewall lo que hace es proteger los servidores y este hardware de acá protege la Intranet. Ahora bien para interconectar esta red porque nuestros servidores deben tener conexión para poder sacar las Bases de Datos, acá tenemos un servidor que se conecta independientemente y hace también firewall – ¿Este servidor donde se ubica? – en la – ¿Pero físicamente? – si físicamente, tenemos enlace acá y para darles Internet a esta oficinas pues se conectan a esta red también, pero ¿qué pasa?, que todos estos equipos tienen dos tarjetas de red, por una se conectan a la red y por otra se conectan a Internet y para no conectar este directamente acá lo hacemos con un xc que no permite compartir información con el Centro de Informática sobre todo, es mas es sólo con el Centro de Informática – ¿Con otras dependencias no? – no, porque nosotros no necesitamos nada de almacén porque ellos son los que manejan la información, entonces las bases de datos las tienen ellos, y bueno esa es la descripción.

Acá tenemos, a este firewall, se conecta también la VIPRI que tiene allá arriba hay otro firewall y esa es la red de la VIPRI – ¿Qué servicios de Internet tienen esas dependencias por Internet pueden hacer descargas, correo, todos? – si todos los servicios, no aquí es una aplicación que me permite controlar los servicios, es

decir puedo yo determinar este equipo puede navegar solo en las páginas de la U o puede salir a Internet, puede tener FTP, chat, telnet y puede utilizar ese servicio de tales horas a tales horas, un sistema, un programa que esta la hora ahí, desde ahí se controla el acceso de todos los equipos que quieran salir a Internet – ¿Esta controlado? – si – ¿a través de que medio de transmisión están conectados? – acá tenemos una red híbrida aquí los enlaces de back-bone de la Intranet usan Fibra Óptica pero también utilizan cable UTP y en algunas aulas, hay dos aulas en las que se utiliza cable coaxial y eso en cuanto a medios de transmisión – ¿Esos medios están certificados? – ¿certificados? o sea lo medios como tal no, lo que se certifica son las instalaciones, no están certificadas. – ¿las conexiones, ponchados, esas cosas se hacen bajo normas? – Si, pues para la terminación de cables se utilizan las normas de la EIA-TIA 568 de cableado certificado o sea todo eso esta montado con… pues basados en la norma no, lo que no esta certificado, es decir lo que no esta certificado para ver si cumple con los parámetros funcionales que exigen las normas, ahí lo único diferente es aquí, aquí utilizamos un anillo de fibra óptica de la RAM de acceso metropolitana que es de Telecom ellos nos prestan un servicio que es desde la Udenar hasta la VIPRI y por ahí nosotros mandamos los servicios es un híbrido aquí se utilizan pares aislados, ah nosotros nos conectamos a Internet con XDSL solo par aislado y Telecom nos recibe ese pack en XDSL y nos entrega nuestro canal que es lo mismo que se utiliza acá esto es XDSL y aquí es XDSL – ¿Qué dispositivos se utilizan en el switch ? – nosotros utilizamos rauter aquí hay un routers, este firewall esta montado sobre un router, este también es un router, acá en la LAN utilizamos switch, solo switches, todo esta con switches ahora y acá en la red de servidores también esta un rack que nos permite el acceso remoto, acceso conmutado del usuario y tenemos en el centro de cableado que es abajo esta el switch hay un switch de fibra Óptica, y la mayoría de los switches son de cobre de UTP para cable UTP.

10. ¿Bajo que parámetros se define la compra de estos dispositivos, entre ellos se establece alguno de seguridad?

No, Realmente lo que prima acá por ser una entidad publica es el precio, acá se le echa mano a lo mas barato, hay equipos de excelente calidad cuando nosotros necesitamos hacer una compra yo presento todas las cotizaciones y las características y cuales son las requeridas pero casi nunca he logrado que me compren lo que yo realmente desearía lo que yo recomiendo, porque el presupuesto es muy limitado, hagamos un ejemplo – ¿Quién determina la compra? – El comité de Sistemas; cuando se va a comprar un switch, la recomendación que hice fue de switches Tricom que permitieran totalmente administrables no tenían manejo de seguridad mentaje lógica de segmentos pero costaban aproximadamente tres millones de pesos cada uno, en cambio la otra opción eran un switch Premium que costaba cerca de un millón de pesos, hacen lo mismo, pero es como complicado.

11. ¿Existe un control sobre el trafico en la red o sea ustedes están revisando si de pronto existe algún sniffer por allí?
Sniffer no, los sniffer son muy difíciles de detectar, tenemos control es de los puntos de la red, es decir todos los puntos que están expuestos al publico pasan por un proxy y el proxy detiene todo tipo de ataques que se puedan intentar hacer a los servidores o pasos a la red de administración e incluso quien quiera salir a Internet, todo se define ahí, pero si hacemos un control de trafico en el proxy, el proxy lo podemos monitorear de donde hay, que cantidad de trafico podemos en determinado instante hacer un análisis de ese trafico para ver que es lo que estan haciendo eso lo hemos hecho para algunos.. ahí estudiantes que son muy curiosos y tratan de violar los sistemas o de pasar, entonces ponen programas que trabajan un poco raros y se los puede detectar y con el sistema de administración se los desconecta de la red, quedan sin ningún servicio; el trafico como tal haciendo controles de ancho de banda también, se hace en este momento estamos acabando de implementar un sistema que permite controlar y administrar el ancho de banda, es decir, un usuario en este momento que se le permita descargas por http, puede descargar lo que quiera al ancho de banda que quiera por ahora no hay controles para eso, en esta semana ya se monta el sistema que digamos, le permite descargar a la máxima velocidad hasta dos megas, pero de ahí en adelante le podemos bajar a 64 K entonces, le podemos decir al equipo que esta en tal ubicación máximo 32 K de velocidad entonces ese sistema se va a aumentar

12. ¿Para el acceso a los servidores que controles se establecen física y lógicamente?
Físicamente los servidores pues están en una oficina que se supone solo tenemos acceso… – ¿Acceso Restringido? – Si acceso restringido pero no es que no haya una gran, digamos seguridad ahí, pues total, tenemos la llave tres personas y desde que se tenga esa llave pues se tiene acceso a las máquinas físicamente.
Obviamente todas las maquinas cuando no están los operadores o nosotros no estamos, permanecen con el lux, la pantalla esta bloqueada no deja la pantalla hacer nada y a nivel de hardware pues hay contraseñas en lo que son PC's en las BIOS, para evitar que los encienda la gente, aunque eso es muy fácil de quitar, excepto en las maquinas, solo en las sparck esas tienen un sistema de protección de open-boot que son contraseñas también y solo la persona autorizada en ese caso yo puedo arrancar ese sistema, pues digamos para otros propósitos porque si se va la energía el sistema baja, cuando llega tiene que subir nuevamente y sin necesidad de dar claves ni nada de eso pero digamos que se necesita arrancar la máquina con otro propósito, por ejemplo recuperar claves o recuperar high-systems, eso si ya requiere una clave que se maneja a nivel de hardware, esa es la actividad física y lógica.

13. ¿A través de las instalaciones, han tenido algún tipo de problemas en cuanto a accesos forzosos?

A las instalaciones, ¿Físicas? – Si ¿porque aquí la seguridad es muy baja? – Si – Fácilmente podrían entrar aunque no tengan llave, podrían romper un vidrio y robar una máquina – Correcto, no nos ha ocurrido afortunadamente, suceden cosas ahora, pero, si es muy vulnerable la oficina ahí donde esta es muy vulnerable, al igual que muchas oficinas donde hay información, nosotros por lo menos solicitamos un sistema de alarma que si se rompe un vidrio, se abre una puerta que, suene una alarma, pero… estamos esperando la respuesta hace como seis meses, mas de seis meses y pedí también un extintor porque no tenemos un extintor, que es básico, no hay un extintor en este edificio, usted busca no y con la cantidad de computadores que hay abajo, se maneja mucha potencia en cuanto a bujías, la posibilidad de incendio es alta, bueno pero es que uno solicita y tiene que estar… es que depende de eso, de la atención que le presten a esa solicitud, yo he hecho la solicitud de todo tipo, de seguridad de acá, de alarmas, de extintores, pero no – ¿Existe control de ambiente en la oficina? – no aun no lo he solucionado, porque como la calor que se encierra es tenaz, eso si nos lo debieron dar de una, un aire acondicionado, pero los purificadores de aire, control de ambiente completo no hay.

14. ¿Específicamente han tenido algún problema de seguridad sea lógico o físico?

Tuvimos en el pasado cuando.. sobre todo desde el Internet, tuvimos ataques desde unas islas, se llama Isla Mabad, eso queda alla en Asia, nos tumbaron un Servidor y la inexperiencia, de ahí en adelante hemos tenido otra cantidad de ataques, ataques se reciben todos los días, desde Internet se reciben aproximadamente a diario digamos unos dos mil ataques, esos están registrados aquí en el firewall ahí ya están bien configurados, ya están digamos que maduros y frenan esa cantidad de ataques, incluso algunos virus es posible frenarlos con el firewall, un virus que por ejemplo de esos que pasan por Internet, ese que apagaba un computador el XP, el caser club, bueno eso no impacta aquí dentro de la Universidad; bueno yo estoy suscrito a un boletín de noticias de seguridad que todo los días le informan por correo que es que ahí, inmediatamente aparece el virus, yo le cerré acá el puesto, por donde él entra, entonces no tiene impacto acá, pero... últimamente no hemos tenido problemas, ataques desde Internet, ataques desde adentro, no, uno solo, fue una estudiante que suplanto la dirección mac del equipo pero con la intención de conectarse a Internet nada mas, pero se le detecto, se le dijo, bueno y ahora ya trabaja acá, pero no ha habido nada grave.

El proxy que tenemos ahora se lo reconfiguro, es hardware nuevo también y esta utilizado para prestar un servicio de telefonía directa para poder hacer llamadas telefónicas sobre la red, eso con el fin de ahorrar llamadas que se hacen dentro, aquí ocurre algo lógico que si usted quiere comunicarse por ejemplo con administración de empresas, con el bloque administrativo, a veces hay que llamar a un número telefónico normal, no por el conmutador, entonces eso es costo, si se quiere comunicar de aquí a la VIPRI hay que marcar a un número, entonces con ese sistema de telefonía entonces le permite hacer esa llamadas por la red y con el computador, ya se han hecho pruebas, ya se sabe lo que se necesita, también

esta hecha la seguridad ahí y yo creo que en unos dos, tres días estamos implementando el sistema control ancho de banda y el de telefonía IP a nivel de servidores, después ya tocaría a cada computador instalarle el software de telefonía.

15. ¿De pronto ustedes manejan políticas internas para lectura de datos, bueno antes de leer algo deben vacunar, tener otro tipo de precauciones?
En las aulas de Informática, no, hay la recomendación de que los estudiantes vacunen sus disquetes, pero así como política no, que sea de obligatorio cumplimiento, no existe – ¿Qué antivirus utilizan? – el que mas se utiliza acá es el Fprot, que es gratis – Es un problema – Si pase un proyecto de licenciamiento de un sistema antivirus para los servidores, es decir proteger desde los servidores toda la red, toca decirles a los usuarios hoy no nos dejen encendidos los computadores para que uno de los servidores se encargue de por la red vacunarlos a todos, etc., pero ese sistema cuesta como cincuenta millones, entonces yo creo que es muy difícil la acogida, pero es un sistema muy interesante, se integra con el correo electrónico, con las descargas, los escaneos de todas las maquinas de la red.

ANX10

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **AUXILIAR DE TESORERIA**

1. ¿Aquí en la Universidad, los han capacitado frente a los procedimientos que se deben tomar en caso de que pueda ocurrir algún desastre o algún inconveniente como un incendio, una inundación o un poco más al extremo algún terremoto por parte del volcán o algo así?
Personalmente se que ahorita, se están haciendo una especie de simulacros, pero ya mas que todo porque empezó a funcionar no de una manera tan efectiva el comité paritario de salud ocupacional pero si ya se esta tratando de implementar, pero, yo sinceramente no se que hacer cuando se presente esto, tocará salir corriendo, por donde uno mas pueda.

2. ¿Cuándo usted tiene algún problema con el sistema hay disponibilidad por parte de los funcionarios del Centro de informática para atender sus necesidades?
Depende de la disponibilidad de tiempo de ellos, a veces es fácil acceder pero a veces por el trabajo, también de ellos como que se dificulta un poco, pero no es lo más frecuente

3. ¿El programa que usted tiene en este momento para su trabajo, cubre todas las necesidades que usted necesita para el normal funcionamiento de su labor?
No, en el momento esta pendiente la instalación de un modulo y de todas maneras como hay enlaces con lo Bancos y esa cosas, entonces los Bancos no envían la información a tiempo, lo cual dificulta de que, por ejemplo un estudiante que haya pagado matricula aparezca como moroso, pero ya él ha pagado en el Banco y el Banco no ha reportado esa información al programa acá a la universidad.

4. ¿Usted ha tenido algún problema en el manejo del programa, que se le dificulte porque es muy complicado?
No, no, los programas son muy bien diseñados o sea son fáciles de manejarlos.

5. ¿Los campos que usted tiene están validados por ejemplo donde van números, sólo le acepta números, donde van nombres, sólo le acepta letras o tiene la flexibilidad de aceptar números y letras?
No, no, si están validados.
.
6. ¿Usted para acceder a su programa, cómo realiza el acceso a través de un nombre de usuario, tiene un usuario o una clave?
Si tengo una clave de acceso, que solamente la manejo yo y el usuario.
.
7. ¿Ustedes realizan cambios periódicos a la clave o es la misma?
Por lo menos trato de hacerlo, frecuentemente cambiar – ¿El programa tiene una opción para realizar el cambio, para que usted pueda realizar el cambio de la clave? – Eso lo hace directamente el administrador del programa – ¿Hay algún mensaje que le sugiera el cambio de contraseña, alguna pantalla? – No, por iniciativa propia

8. ¿Frente a la capacitación, a usted le han dado la capacitación necesaria para el manejo del programa?
De todas maneras, no, de pronto se me facilita un poco porque tengo una tecnología en administración Informática y soy técnico en sistemas, por eso se me facilita un poco pero así que se hayan sentado a decirme esto, esto, no, si no que ya por la misma experiencia, pero realmente si se hace necesario, no solamente la parte operativa si no de manejar lo más eficiente el programa.

9. ¿Usted cuenta con un manual del programa?
No, eso es una falla que tenemos, no tenemos ni de administrador del programa, ni manual del usuario, no hay.

10. ¿De pronto por la carga que tiene de trabajo, pueda tener algún problema por estrés o algún problema físico?
Claro, eso si, sobre todo ahorita por ejemplo en lo de matrículas, entonces la carga de estrés que se maneja es impresionante por las liquidaciones que son mil quinientas, que entran a primer semestre, más los profesionales, las liquidaciones que hay que hacer de esas matrículas, entonces es bien complicado

11. ¿Para ingresar la información al sistema, tiene algún formato en especial?
No, o sea la forma está, pero necesariamente hay que capturar los datos a través de un formulario y meterlos acá – ¿Esos formularios se encuentran de pronto numerados en consecutivos? – Por ejemplo en los embargos, esos salen con la nómina o sea yo pienso que no, la nómina del mes de junio se graba en lo embargos del mes de junio, los formularios de inscripción vienen numerados, unos por fecha y otros por número de pronto se genera un control, un consecutivo

12. ¿Se revisa por ejemplo, que los formularios estén sin tachones, enmendaduras o que no le haga falta información antes de ingresarlos al sistema?

Pues sobre todo en lo de matriculas, si el estudiante no presenta la información es perjudicial para él porque, es un sistema, la matricula por decir algo tiene un costo de tres millones, pero si el estudiante presenta el estrato, le va a rebajar, si el estudiante, presenta los ingresos le va a rebajar, si el estudiante dice que es colegio público o privado, si es de público, pues le va a rebajar, entonces esa información que tiene que darse y si no presenta ningún papel, entonces le sale la más alta, entonces de todas maneras, si se presentan errores y los tachones y esas cosas – ¿Y esos documentos, se los devuelven al estudiante? – No, esos quedan archivados acá.

ANX11

ENTREVISTAS CON EL PERSONAL DE OCARA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **AUXILIAR DE REGISTRO ACADEMICO DE POSTGRADOS**

1. ¿Qué funciones le implica su cargo?
Matrículas de pregrado, postgrado, información general en ventanilla y todo lo que tiene que ver con hojas de vida de estudiantes

2. ¿Sus funciones corresponden a las establecidas en el manual de funciones?
Si – ¿Existe este manual? – No para mi cargo

3. ¿En lo que se refiere a seguridad física, se han realizado dentro de la Universidad de Nariño planes de emergencia y evacuación en la que la dependencia haya participado?
En ningún momento – ¿Directamente usted? – No, nunca, en ningún momento – ¿Alguna sugerencia al respecto? – La Universidad de Nariño, involucra todas las dependencias, se sabe que OCARA, es la dependencia mas importante de la universidad, pero nunca se la tiene en cuenta para este tipo de procesos – ¿Personalmente conoce el procedimiento a realizar frente a posibles desastres, como incendios, terremotos? – En absoluto, esos planes de emergencia y evacuación, en la época del volcán Galeras, se realizó por parte de un equipo de trabajo me imagino que haciendo alusión a este problema, pero nunca se tuvo en cuenta a la oficina de OCARA, se tuvo en cuenta otras dependencias, otros edificios, pero a OCARA, la borraron de la planta física de la Universidad, de hecho, si borraron una oficina, con mayor razón borraron al personal, no se lo tuvo en cuenta para nada de lo que estaban haciendo.

4. ¿En lo que se refiere al desarrollo del software, hay disponibilidad por parte del Centro de Informática para atender sus necesidades e inquietudes, acerca de la aplicación que manejan?
El centro de Informática es una dependencia de la Universidad que maneja muchas cosas y por el volumen de actividades que realizan, en su momento cuando se le presentan problemas a uno, no se lo solucionan de ya, si no lo dejan, esperemos para mañana o te mandamos a un monitor del aula, cuando son cosas demasiadamente urgentes, entonces toca que estar llame y llame, pero de pronto

no es porque la entidad o la dependencia no pueda arreglarlos, es por el innumerable número de actividades que ellos realizan, que el personal no es suficiente para atender las necesidades que nosotros desarrollamos o que tenemos.
5. ¿El sistema actual cubre las necesidades en cuanto a los procesos que maneja esta dependencia?
No, obviamente se esta tratando de implementar un nuevo paquete, porque el volumen de estudiantes ha crecido tanto y el sistema es tan "pobre", pobre, no se muy bien, pero exige muchas mas tecnologías que la universidad todavía no las tiene, hay muchas lagunas, hay muchas necesidades de los estudiantes que hay que solucionárselas de inmediato y que sólo la tecnología bien aplicada se puede solucionar este tipo de problemas, se esta trabajando en eso tengo entendido que la universidad compró un paquete de informática para poderle solucionar esto a los estudiantes, pero ojala que con ese paquete si se puedan suplir todas las necesidades de los estudiantes.

6. ¿Ha tenido algún problema en el manejo de estos programas?
Particularmente, mi cargo que desempeño, no requiere tanto el manejo de paquetes para los estudiantes como los que manejan las auxiliares, en mi caso no tengo problemas con mi paquete

7. ¿Ha tenido inconvenientes para ingresar datos al sistema?
No es mi labor ingresar datos al sistema.

8. ¿Respecto al control de acceso, entra al sistema a través de un nombre de usuario y una contraseña?
Si, el Centro de Informática nos da una contraseña – ¿Se evita la visibilidad de la contraseña en la pantalla? – En algunas cosas, en algunos programas para entrar, en otros, si se ven los paswords – ¿En qué programas? – por ejemplo para entrar a constancias, si se ven los paswords.

9. ¿Se realzan cambios de contraseña de manera periódica?
No, en mi caso no, llevo trabajando más de seis años con la misma contraseña

10. ¿Cuál es el procedimiento que se hace para realizar el proceso de cambio de contraseña?
Con Centro de Informática, pidiendo autorización o que uno de los señores, de los ingenieros que trabajan allá, nos la cambie – ¿A petición del usuario? – A petición del usuario

11. ¿Dentro de su menú de usuario existe una opción para el cambio de contraseña?
No, en absoluto.

12. ¿En algún momento el sistema le esta haciendo mensajes en que sugieran el cambio de contraseña?

No, en mi caso no

13. ¿Por parte del Centro de Informática, ha recibido la capacitación necesaria para el manejo de los programas?

No, de ninguno

ANX12

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **SECRETARIA DE ALMACEN**

1. ¿Su función es trabajar con Inventarios?
Con inventarios – ¿Realiza la digitación? – Al comienzo yo los digitaba pero después hace seis años, ya se sistematizo entonces, carga la compañera, carga ella y simultáneamente como ella va cargando, va pasando aquí al servidor – Claro como están en red. – Si estamos en red, entonces, lo único que yo ahora, ya es revisar, revisar todo, todo lo de la universidad, estoy revisando, corrigiendo, haciendo traslados, cuando aparecen pérdidas, revisar porque se hizo, todo lo de inventarios y cada año se realizan los inventarios en cada dependencia, en cada dependencia se los imprime por secciones y se va a la dependencia para ver en que situación se encuentran, luego se hace firmar, ese es el trabajo, estar pendiente, estar pendiente de los cambios, ah de los equipos nuevos que llegan, ver quien los tiene, quienes son los responsables, quien los va a utilizar.

2. ¿Respecto al programa que utilizan realmente si cubre todas las necesidades que tienen para realizar el procedimiento de Inventario?
Bueno a nosotros lo que nos enseñan es a manejarlo – ¿no han tenido problemas? – Si hay sus problemas, si hay sus cosas que resulta que a veces se cambian, por ejemplo lo de inservibles, no aparecen, se duplican, entonces ya viene el Ingeniero de sistemas y lo arregla, no se que es lo que le hace, pero eso es problema de nosotros

3. ¿Respecto a la disponibilidad de parte del Centro de Informática para atender cualquier problema que tienen la atención es inmediata, cual es el procedimiento que realizan ustedes para hacer la solicitud?
Bueno, nosotros cuando hay problemas, si el Ingeniero de Sistemas que es Henry Rodríguez, él viene, si el es una persona bien amable, bien accesible y por lo tanto… si viene cuando lo necesitamos con urgencia el esta pendiente, el llega – ¿De pronto como validación que le hacen a los datos en lo que se refiere de pronto a los formatos de fecha, usted esta de acuerdo con esa validación o ha tenido algún problema, para el ingreso de datos, las validaciones que realiza? – Allí si no podría decirse porque pues como allá cargan, allá dependen las fechas

con las fechas ¿será eso que cuando cargan..? Cuando entra el equipo pues el elemento entra en las facturas aquí, a veces… hay equipos que no aparecen y en las dependencias aparecen los equipos pero es porque no han legalizado con el almacén, no han legalizado, entonces nos toca a nosotros ir a buscar, a investigar porque no entro este equipo aquí en almacén, porque no se presentaron los papeles, porque hay dependencias, hay funcionarios que reciben los equipos y no los legalizan, allí a veces hay descuido.

4. ¿Respecto al control de acceso que usted tiene al sistema usted entra al programa a través de un nombre de usuario y una contraseña?
Si, si nosotros tenemos una clave y entramos con esa clave, ya seguimos – ¿mientras usted esta digitando la clave, esta aparece visible en la pantalla o es oculta con asteriscos o simplemente no aparece? – No, todo aparece, si todo – ¿pero si se ve la clave, su clave? – Es decir…haber no, entonces esa clave… antes había clave pero yo no tengo clave, no se porque no le han puesto, ni le he dicho yo a Henry que me coloque una clave porque hay veces que han venido, que uno nota que el computador no ha sido apagado como debe ser, correctamente, entonces no… hay siempre, entonces yo le he dicho con una clave, ponga una clave, pero entonces no, no la ha puesto – ¿Usted no tiene aquí la posibilidad de cambiar clave dentro del menú de la aplicación? – No, no

5. ¿Para la parte del Centro de Informática, pues en el caso suyo no, pero para las demás, están sugiriendo el cambio de contraseña o ustedes solicitan el cambio de contraseña?
Nosotros cuando hay necesidad si pedimos, pero otra cosa, yo no le puedo poner clave ni nada porque este es el Servidor, entonces, y que tal el Servidor con clave y el día que yo no este no pueden trabaja los otros – ¿esa es la razón? – si esa es la razón.

6. ¿Respecto al entrenamiento, usted recibió la capacitación necesaria para el manejo del programa por parte del personal del centro de Informática?
Si, si nos dieron una capacitación.

7. ¿Usted cuenta con un manual de Usuario para el manejo del Programa, les dieron esa información o un manual?
No nosotros por ahí con ellos nos dictaban el curso, luego ellos venían a indicarnos, a enseñarnos como debemos manejar

8. ¿Usted siente que por carga excesiva del trabajo le pueda originar efectos de estrés?
Si esto es lo más estresante, es que es un trabajo muy estresante, no, no entre todos que uno no cuenta con funcionarios, que a veces cuando uno va a verificar no tiene esa colaboración y a veces dicen no las cosas aunque estén, No, no están, pero uno no puede llegar y buscar así eso no da con el inventario siempre uno se siente mal, es estresante, es complicado, es muy estresante, cada año es

no, no y todo el tiempo me toca, todo el año tengo que estar dele y dele acá, cambie y cambie, traslados, no…ese es el trabajo

9. ¿Ustedes tienen formatos preestablecidos aquí en la dependencia de almacén para el registro de los datos, tienen algún tipo de formato para trabajar inventario, ingresos, egresos?
Si tenemos un formato de inventario, imprimimos el inventario y nos sale ahí todo y con base en esa inscripción nosotros vamos a hacer la… a estar informando, ahí sale a nombre de quien, quien es el responsable la dependencia, todo, es un formato bien adecuado y entonces cuando ya cambian los funcionarios hacemos firmar quien entrega y quien recibe – ¿Y estos documentos se controlan con numeración consecutiva? – No, se controlan con número de secciones, código y sección, cada sección tiene su número de código – ¿pero si se identifica por decir algo, que un dato, un papel no se duplique, pase alguno, existe algún control sobre eso? – Hay actas, si, las actas de entrega, esas actas de entrega van enumeradas, si esas si van enumeradas, esa es la base para nosotros establecer responsabilidades, con esa acta, quien firma el acta tiene que responder.

10. ¿Ustedes revisan los documentos que no tengan tachones o enmendaduras o espacios en blanco que sean obligatorios de llenar, se revisa todo?
Si todo eso es firmado, revisado y por lo regular nunca no… porque pues nosotros sabemos como somos.

11. ¿Para el ingreso de datos al sistema, que cuidados se tiene para no cometer errores de digitación o posteriormente a esto se hace alguna revisión?
Por lo regular los datos los carga la compañera, pero cuando a mi me toca cargar los datos, yo reviso bien, miro a que código pertenece, la persona, la persona con su respectiva cédula, la dependencia, el valor, todo, si lo reviso

12. ¿En cuanto a seguridad física, usted conoce algún procedimiento o los han entrenado frente al procedimiento que tiene que realizar ante posibles desastres dado el caso que se aquí se presente una inundación, un incendio, un terremoto, ustedes tienen conocimiento de ese desarrollo durante la actividad?

.No, nunca, nada, nada, lo único nosotros que tenemos es aquí es una cinta de seguridad, lo único, el backup, que nos toca sacarlo cada…, pues yo lo saco cada quince días el backup, es un backup que existe, esa es la única seguridad que tenemos no hay más – ¿cada cuánto realizan copias de seguridad? – yo las realizo cada quince días, cada quince, cada que tengo tiempo, yo no tengo tiempo

de estar… aquí es contado – ¿Y en dónde guardan esa copia? – Yo la guardo en mi escritorio – ¿aquí en la Universidad? – Si, pero también esa cinta de seguridad la tiene el Ingeniero de Sistemas, él la tiene – ¿Henry? – Si, el también tiene, el también saca.
Verá no, la Universidad, el almacén lo tiene como en último, digamos aquí donde se lleva el control de los bienes de la Universidad debería haber una seguridad, aquí en servicios generales, aquí cuando nosotros no venimos a trabajar los Sábados y Domingos, parece que usaran los computadores, que yo creo, yo creo que aquí debería haber es decir… o no se, establecer una seguridad especial para los equipos, todo, un control de acceso porque aquí entra todo mundo y el almacén es relegado, el almacén es lo último, es ultimo, la Universidad no lo tiene en cuenta para eso, para nada, para nada. – ¿Qué control, se tiene aquí sobre la llave, todos tienen llave o quien tiene la llave? – la llave de una sola puerta que hay entra… para funcionarios de servicios generales, aquí entran choferes, conserjes de todo y para nosotros, pero yo pedí el almacén independencia, aparte que cada funcionario del almacén tenga su llave, pero aquí no, tiene acceso todas las personas.

13. ¿Dentro de la dependencia de aquí del bloque donde funciona almacén ha habido pérdida de equipos?

No, aquí dentro de almacén, no, pero sí, de las otras dependencias, en sentido por ejemplo, se pierden de VH's, grabadoras, aquí dentro de almacén no, pero en toda la Universidad si hay pérdida.

14. ¿Cuando han realizado las tomas del bloque, cuando hay paros, aquí hubo pérdida de algún elemento?
Aquí en el almacén no, pero si en otra dependencia donde hubo, por ejemplo donde permanecían los estudiantes, si hubo informe de pérdidas, pero perdidas no muy grandes, pues a mi no me consta que se perdieron los discos duros de los equipos, pero mas no así que se digan equipos grandes no, pero las otras dependencias si se han perdido grabadora, VH's, me parece que eso es por descuido – ¿no existe un control sobre eso? – no, antes de nosotros manejar los inventarios, se perdía mucho, pero como ahora hay un control – ¿Existe un responsable? – Eso, entonces uno va ya y si usted saca esto, tiene que responder, tiene que reponerla.

ANX13

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **AUXILIAR DE CONTABILIDAD**

1. ¿En lo que se refiere a seguridad física, usted conoce algún procedimiento o sea han realizado procesos de evacuación frente a desastres?
Una evacuación no – ¿O que hacer en un caso, por ejemplo, aquí como estamos cerca al Volcán Galeras? –.No, no hemos recibido ninguna capacitación – ¿Ningún desastre de incendios? – ni incendios, ni nada, no hemos tenido nada.

2. ¿Cuándo ustedes tienen requerimientos para el programa, tienen necesidades que cumplir, hay una disponibilidad inmediata por parte del personal del Centro de informática?
Hay un compañero que trata de colaborarnos, lo mejor posible, en algunos momentos, a veces no se lo encuentra porque esta en otras dependencias, pero generalmente digamos que si es favorable, la atención del compañero que esta a cago del equipo de contabilidad, el si tiene disponibilidad para colaborarnos, sin embargo aquí en la oficina, también tenemos un compañero que es Ingeniero de Sistemas, cualquier cosita, primero nosotros acudimos a él, cuando se trata de sistemas, cuando ya se trata del programa, vamos al Centro de Informática

3. ¿El programa que tienen actualmente, realmente cubre todas las necesidades que existe en esta dependencia?
En este momento, no nos cubre todas las necesidades porque, especialmente lo que nosotros necesitamos es una integración, empezando porque se repite mucha información, mire todo esto que tengo que mensualmente hacer esta consolidación, perfectamente podríamos nosotros sacarla del sistema y no tenerla que hacer manual, como se la esta haciendo, en realidad el sistema no nos cubre todas las necesidades

4. ¿Ustedes han tenido algún problema respecto al manejo del programa?
No, el manejo del programa es muy accequible, es muy fácil de manejarlo, el programa es fácil manejarlo, pues poniéndole su poquito de interés, no se dificulta.

5. ¿Han tenido algún tipo de problemas con la validación de los datos del programa, puede ser de codificación, de fechas, existen estas validaciones?
No existen validaciones, existen validaciones pero ya de otras entidades, sin embargo aquí interno de nuestro trabajo diario, no existe una validación – ¿El programa, le indica por ejemplo que puedan tener algún tipo de inconveniente, en casos donde usted tenga que poner por ejemplo sólo letras o sólo números, que le permitan, de pronto una cédula vincular una letra o un carácter que no sea un número o eso lo maneja correctamente donde sólo van número, únicamente les permiten meter números? – No siempre esta números y letras, porque por ejemplo en la codificación del presupuesto, la codificación del presupuesto llega un momento en que si el parámetro que nos deja… nos permite ya poner un a o un b y lo hemos hecho perfecto, permite yo creo que alfanumérico, y no debería ser eso, no debería ser, porque se prestaría a errores de digitación.

6. ¿En lo que se refiere al control de acceso del programa, usted entra a través de un nombre de usuario y una contraseña?
Si tenemos nuestra clave, eso ya depende de cada quien, en realidad ya hemos ido donde el compañero del centro de informática, porque anteriormente no teníamos esa clave, cualquiera podía entrar al programa, pero a raíz de algunos problemitas que se nos presentaron, porque siempre, no hubo voluntarios, errores involuntarios en que algunas compañeras entraban a digitar, se equivocaron de fecha y como el sistema acepta eso, yo hoy puedo perfectamente hacer un movimiento un registro con fecha enero, con fecha febrero, que eso es algo que estamos tratando de… porque se nos han presentado problemas por eso, de que a lo dos, tres años por error alguien en vez de colocarle 2004 le coloca 2002, se nos hace el registro de años anteriores y a raíz de eso solicitamos que a cada uno, se nos diera una clave.
.
7. ¿Usted maneja, por decir algo una política en el que se realice cambio de contraseña periódicamente?
No, yo desde que la tengo, tengo la mima contraseña, que podría ser, tal vez ya sería cuestión de que no hemos ido donde el compañero para que nos la cambie, pero tampoco ha habido la sugerencia de allá, vengan cambiemos – ¿El sistema en ningún momento realiza mensajes en los que sugiera cambios de contraseña? – No, en ningún momento – ¿ustedes en el menú de usuario tienen la posibilidad de cambiar la contraseña o viene directamente del Centro de Informática? – Directamente del Centro de Informática.

8. ¿Referente a la capacitación que ustedes han tenido para el manejo del programa, considera que ha sido suficiente la capacitación por parte del Centro de Informática?
Pues hemos recibido las especificaciones correspondientes para el manejo, sin embargo no tenemos una amplitud cuando uno quiere ya salirse o necesita salirse de los parámetros, estamos como muy limitados, entonces ya nos toca acudir a ellos y en ocasiones que el compañero no esté y que este prestando atención en

otra dependencia, uno tiene que esperarlo hasta que llegue, entonces, yo creo que nos hace falta como un poquito más de flexibilidad, que uno pueda tener mas entrada al sistema, que pueda, cualquier cosita que yo necesito, cambiar un listado, sacarlo aquí, sacarlo acá o hacer una corrección de pronto… hacerlo más directamente

9. ¿Por parte del Centro de Informática, a ustedes les han facilitado el manual del usuario del programa de manera que los oriente sobre el manejo del mismo?
No, en ningún momento, no tenemos conocimiento.

10. ¿Respecto al trabajo que usted tiene, usted considera que es demasiada la carga que tiene de manera que le pueda ocasionar efectos de estrés?
Si, en realidad yo estoy recargada de trabajo al punto de que yo estoy llevando trabajo a mi casa, claro que tengo aquí el tiempo completamente copado, hay días que es mas porque mi cargo es como para presentar informes, me solicitan continuamente y yo tengo que estar pendiente, me toca hacerlo a Contraloría, los informes a Contraloría y en este momento ya nos solicitaron también, informes de la contraloría nacional o sea que es a las dos contralorías, en realidad si estoy como un poquito recargada de trabajo.

11. ¿Para el registro de los datos, ustedes ya tienen unos formatos preestablecidos?
Si, en realidad se ha tratado de ir nosotros mismos haciendo nuestros formatos, lógicamente si hablamos de registro, por ejemplo un registro presupuestal eso ya el sistema nos lo da, pero si hablamos de otra clase de registros, consolidación que se me presenta así, que lo hago yo en Excel, si son los de contraloría, esos ya tienen sus propios formatos donde nos toca llenar datos y la dificultad aquí es de que aunque en el Centro de Informática no han colaborado tratando tal vez de hacer una homologación de códigos porque Contraloría pide unos…nosotros partimos de unos códigos del estatuto presupuestal, Contraloría pide otros códigos y Contaduría pide otros códigos, entonces imagínese que uno trabaja con varios códigos, pero hasta el momento no ha sido posible a pesar de que eso códigos se los ha digitado, no ha sido posible, ya que la información sale directamente del sistema, nos ha tocado hacerlo en una forma muy manual y otro problema que se presenta es cada que sube un contralor tenemos completamente cambio de presentación de cuentas, ahoritica estamos esperando en la Contraloría departamental a ver cómo es que vamos a presentar esos informes, eso siempre requiere otra vez de tiempo porque toca hacer una homologación, analizar como es que se da la nueva información, es un poquito complicado.

12. ¿El control de estos documentos, de estos formatos, se realizan con una numeración consecutiva?

Para el registro presupuestal si, ese lleva una numeración consecutiva y todo parte del certificado de disponibilidad que también viene con su numeración consecutiva, entonces el registro lleva el mismo número de disponibilidad, el número de disponibilidad lo utilizamos para el registro, para la obligación, para el pago y el registro también, como ese se lo imprime, ese también lleva una pequeña numeración – ¿Se revisa que los documentos, en ningún momento tengan errores, que tengan tachaduras o espacios que sean de obligación de llenar, que estén en blanco? – No, porque esos ya salen directamente del sistema, o sea que se llena ciertos datos y el resto, el mismo sistema automáticamente nos los llena

ANX24

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **DIRECTOR DE TESORERIA**

1. ¿Cuándo se hace un desarrollo de los programas que manejan aquí en la dependencia de Tesorería para ese proceso de la construcción de los programas, hay participación por parte de los funcionarios de las personas que operan esos programas?
Si, Indudable porque no puede haber desarrollo de programas si no hay participación de los usuarios – ¿Y es activa la participación? – Si, es activa, el problema es que todo tiene su... o sea yo soy partidario de la participación activa de los usuarios por una parte, pero por otra no es suficiente no es del todo acertado en este sentido, resulta que si se quiere hacer una reingeniería de procesos no se puede confiar en la participación activa de los usuarios, ese ha sido el problema, nosotros hemos tratado de modernizarnos, pero siempre nos preguntan a nosotros y nosotros tenemos la concepción de lo antiguo, de cómo esta funcionando, así este funcionando mal y así queremos que siga funcionando, entonces, es como todos los procesos, si uno quiere avanzar tiene que romper, ser revolucionario y eso tiene que de pronto irse encima del querer egoísta de las personas, de lo seres humanos es una cuestión de metodología, tiene que haber participación, pero tiene también que haber un desarrollo, una concepción global, qué queremos hacer, qué vamos a hacer con los proceso contables, administrativos y financieros, de ahí debe partir toda la filosofía, pero si nos ponemos a consultar qué quiere el cajero, el cajero quiere seguir trabajado como ha venido trabajando los últimos años, la señora de bancos quiere seguir trabajando como ha trabajado los últimos años, porque ya se acostumbro a ese proceso semi-manual, semi-automático que estamos trabajando en este momento, todo lo que sea modernizar por lógica, por nuestra naturaleza humana choca con nuestra seguridad porque ya se nos ha acostumbrado a los procesos que ahí, o sea, en realidad informática si nos participa a nosotros de los proceso, pero a veces yo objeto eso porque quisiera que hubiera alguien que ya tiene experiencia en eso que expusiera unos procesos que mejorarán lo que existe.

2. ¿Existe algún documento o usted diligencia algún documento para solicitar que se hagan servicios por parte del centro de informática o lo hacen vía telefónica o como se realiza?
No, eso se realiza personalmente, resulta de que ya puedo hablar porque ya estoy de salida, aquí en la Universidad de Nariño hay un tabú por lo escrito, si uno escribe algo la gente se siente ofendida, por ejemplo, si yo le pido un favor a Informática por escrito, ya se duelen, porque no vino a hablar conmigo, si podía hablar conmigo, entonces es imposible hablar de escritos en la Universidad, si uno le dice a un jefe por escrito algo, se siente ofendido y ya lo trata a uno de desleal, entonces es mejor, todo toca personalmente y lo malo es que lo personal se olvida, se niega, entonces no queda ningún registro escrito, es algo ilógico en el área administrativa, la primera empresa en la que yo veo, que escribir ofende a la gente y la ofende mucho se sienten en su ego, entonces vale mas lo personal lo egoísta, que lo institucional, esa es la verdad.

3. ¿Una vez terminado el proceso de desarrollo de los programas son los usuarios de la dependencia de tesorería quienes realizan pruebas a esos programas que se han desarrollado o los programas ya vienen probados?
Si, afortunadamente, en medio a veces del desorden que yo observo, hay personas en Informática que se preocupan por conocer de los procesos, entonces yo he visto los programadores de allá de Informática, ellos saben que hace cada uno de los usuarios entonces, conocen, son capaces en un momento dado de reemplazarlos porque ellos han trabajado en esto, entonces ellos prueban los programas y luego los traen acá, si hay que hacerle un ajuste, en ese sentido ha habido mucha colaboración.

4. ¿Existe un documento sobre el cual se apruebe a conformidad el desarrollo del programa que se están entregando?
No, no, la parte documental es cero, no existe.

5. ¿Existe exactitud en lo procesos que realizan los programas o tiene problemas de inexactitud que no le cuadra alguna cuenta o problema de ese tipo o que se duplican los datos?
No sabría decirte, o sea, seria arriesgado decir que eso ha pasado, seguramente que hemos encontrado alguna cuestión así, pero puede ser por error de digitación, pero seria arriesgado decir que si, que se esta duplicando información

6. ¿Considera que son adecuados los recursos tecnológicos por parte de comunicaciones, en equipos de cómputo con los que cuenta en este momento la dependencia?
No, no son adecuados, precisamente esa ha sido una lucha aunque la concepción que tienen quienes están tratando de implantar un sistema de información adecuado es primero tener un sistema y luego equipar, claro que esa es la lógica, pero en este momento no, estamos todavía trabajando a retardo como hemos comentado en anteriores oportunidades son programitas para un usuario otro

programita pero redes no existen, por ejemplo aquí hablan de convenios, se abren cuentas nuevas y nosotros no nos informamos de que convenio hay porque no hay sistemas de información, debería haber una base de datos integral, a la que puedan acceder lo interesados, como interesado ahí mucha información que no tengo acceso y que me afecta y afecta al desarrollo de la oficina.
7. ¿Usted dice que los procedimientos para comunicarse con el Centro de Informática son verbales?
Son verbales, si o sea, mas basados en la amistad personal que no…no por los funcionario que son los que trabajan, sino por la parte administrativa, la burocracia si se les escribe vienen modestísimos, o sea, uno cerro sus puerta para la solicitud, si uno escribe.

8. ¿Cuando se solicita algún servicio al centro de informática, los funcionarios del centro de informática responden con puntualidad a los requerimientos?
Si, pero todo toca verbalmente y basado… el principio debe ser la amistad, la solicitud respetuosa, verbal porque – ¿Tienen que haber buenas relaciones? – Si, eso tiene que ser primordial, eso va por delante.

9. ¿Usted revisa y acepta la información que se va a ingresar al sistema o directamente la ingresan los operarios?
Si, los usuarios, ellos tienen la autonomía para ingresar la información, claro basado en documentos reales, legalmente, por ejemplo hacen cheques basados en las ordenes de pago, entonces se ingresa la plata con el efectivo, los recibos de ingreso son con el efectivo, efectivo y cheques que entren por caja.

10. ¿Los reportes que produce el sistema, reporte de bancos, reporte de caja los revisa usted como director?
Si, claro yo le reviso diario, diariamente, el Boletín diario.

11. ¿Existe un responsable de la llave de acceso a las instalaciones de esta oficina?
No, en realidad en eso si ha habido democracia, el que llega primero, abre – ¿todos los funcionarios tienen llave? – Si, todos tienen llave.

12. ¿Hay un horario interno a nivel de la dependencia, un horario de trabajo establecido o se sujetan al normal de ocho a doce y de dos a seis?

De dos a seis, ese es el normal, inclusive, últimamente hay la política.. el portero viene prácticamente lo saca a uno a empujones a las seis de la tarde, a las doce

del día si uno no…– ¿Sale? – Si, y si hay alguna cosa, el jefe de sección debe pedir autorización para quedarse, al funcionario – ¿a quien pide esa solicitud? – Eso ha ido cambiando últimamente por aquí tenia una circular donde se prohíbe el acceso, el Jefe de Planeacion pedía autorizar, últimamente para que se quede un funcionario en alguna dependencia, hay que pedir permiso al jefe de Servicios Generales para que él le informe al portero, al celador que uno se va a quedar trabajando -- ¿Por parte de quien viene esa circular? – de Rectoría, eso tiene un origen plausible, pero a veces un resultado perverso, el origen es que mucha

gente se quedaba haciendo trabajos personales en lo equipos y eso si esta prohibido y debe ser así, es lo que tengo entendido, equipos, teléfonos, hacían llamadas después de las seis, después de las doce, se quedaba gente y hacia llamada personales de larga distancia, pero entonces el problema es que por ejemplo yo tengo a veces nómina y son las seis y nos vienen a sacar y entonces a uno le da rabia y se sale, así se quede todo a mitad de trabajo, si porque mirar que un chafarote, porque ahora han contratado a unos estilo militar y entonces ellos vienen y lo sacan y yo como detesto a los milicos ¡Bueno ya me voy! y en estas circunstancia de mi vida que uno tiene los afectos por quien mal lo trata, entonces no, si mejor, o sea la orden tiene un origen valido, esta bien que se quede la gente trabajando pero tiene que quedarse trabajando en lo que son sus labores no en otras labores, se quedan haciendo sus trabajos de grado, imprimiendo, fotocopiando, haciendo cosas así que no corresponden, haciendo llamadas

personales a los hijos, a los estudiantes, entonces eso había que acabarlo y eso esta bien.

13. ¿A nivel interno de la dependencia, existe algún control sobre la circulación de equipos, o sea, se pueden mover lo computadores libremente?

Ah si, porque el responsable es el tesorero de todos los equipos, hasta de la última regla**…** – ¿Dentro del inventario? – Dentro del inventario, si puede haber movilidad, este equipo, me lo acaban de pasar y lo tenía la señora de bancos – ¿Pero entre ustedes no tienen responsabilidad sobre los equipos, por decir tal persona se encarga de...? – Si, eventualmente le ponen, pero quien firma todo el todo el inventario es el jefe ha habido vaivenes en eso porque como no hay escrito nada sobre normatividad, entonces, hay veces que me ponen todo el inventario a nombre mío, hay épocas que lo ponen… vienen y dicen usted tiene un computador, esto es una regla, una cosedora, una perforadora entonces le van cargando personalmente, otras hacen un solo inventario y lo firmo yo, por eso no ha habido problemas aquí, porque son personas que llevan muchos años – ¿Y a nivel Interno usted maneja algún registro de las personas que tienen, que computador, que equipo? – No, no, en realidad no, no existe eso – ¿Se prohíbe el uso de cigarrillo, el consumo de cigarrillo a nivel interno de la dependencia? – Si, o sea afortunadamente no hay ningún fumador acá, no hay fumadores – ¿y el consumo de comestibles o líquidos cerca a los computadores? – No, en eso en realidad no hemos sido estrictos, no porque no…es tanta la pobreza en la Universidad, no tiene ni azúcar, ni tinto para darnos a nosotros, entonces en realidad cuando traemos nuestro tinto cada uno lo hace a veces, en su termo o tenemos una cafetera y se hace café en la cafetera pero se toma en el punto, en el sitio de la cafetería – ¿cerca a los equipo no? – No, no

14. ¿Existe un mantenimiento periódico a los equipos por parte de alguna de las dependencias?
No, no hay un mantenimiento, un contrato, por lo menos yo no lo conozco, pueda que haya a la central llegue, pero en si yo no he visto – ¿o cada que se daña un equipo? – Si, entonces nosotros llamamos y entonces… – ¿correctiva la cuestión? – Si es correctiva, no es preventiva es como la salud de los colombianos, que solo cuando estamos enfermos vamos al médico.

ANX25

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **JEFE DEL DEPARTAMENTO DE CONTABILIDAD**

1. ¿En el momento en que se hacen programas o se ha desarrollado programas por parte del centro de informática, para la dependencia, ustedes han participado en el proceso de la creación de estos programas de manera permanente, mirando que requerimientos se necesitan, apoyando a los programadores del centro de informática en el desarrollo de los mismos programas?
Yo pienso que esta parte no ha sido muy eficiente, digamos, si bien es cierto ellos han desarrollado sus programas y no has pedido pues opiniones y todo eso pienso que no ha sido muy bien el… claro, esa relación que se ha mantenido – ¿Han tenido ciertos inconvenientes?– Hemos tenido varios inconvenientes – ¿Alguna referencia? – Yo pienso que mas que todo nos ha faltado es como ese apoyo tan directo de parte de sistemas porque si bien es cierto ellos dicen que nosotros somos los que tenemos que decirles todo lo que queremos y como salimos pero en muchas partes o nos dicen bueno ustedes cómo quieren que se haga la información, que resultados, nosotros si lo decimos, pero si nos dicen también cómo es que ellos tienen diseñado y qué campos tenemos que llenar, si ha faltado definitivamente esa buena relación entre las dos dependencias.

2. ¿Cuándo se van a hacer unos requerimientos, se van ha hacer solicitudes de servicios para gestión de programas u otro tipo de servicios, al Centro de Informática, esos requerimientos, esas solicitudes se realizan por escrito, verbalmente, vía telefónica, como se hace?
Algunas veces por escrito, pero la mayoría de las veces hablamos con Fredy, que es el que maneja todos esos programas y él empieza a trabajarlos, viene y nos pregunta y nosotros le decimos, así es como ocurre.

3. ¿Una vez terminado el proceso de creación de los programas, el Centro de Informática, viene, entrega el programa aquí a la dependencia, los usuarios de esta dependencia realizan pruebas a esos programas o los programas vienen ya probados y ustedes comienzan únicamente a ingresar datos?
Por lo regular, ya sobre la marcha es que se va corrigiendo o sea se instala un programa y de pronto empezamos a ver que mire que falto esto, que mire que lo

otro, o sea algunas veces se hace una prueba, pero otras veces es sobre la marcha que se van corrigiendo – ¿A partir de la entrega que le realizan? – Si, van resultando muchas cosas que de pronto no están, es el problema que tenemos ahora con Tesorería que no se puede crear, ustedes saben, unos rubros, que no se pueden crear que porque el programa ya esta así, bueno no sé, hemos tenido una cantidad de inconvenientes en ese sentido como que no es bien flexible, que después para que nos hagan ya eso, ya hay que diseñar otro programa, que por qué no lo dijeron antes, empieza ese contrapunteo por la misma falta de buena relación, que ha existido – ¿Buena comunicación? – Si digamos que es comunicación.

4. ¿Existe un documento en el cual se apruebe a conformidad el funcionamiento de los programas, un documento para que usted legalice, es decir, estamos conformes…?
No, yo nunca he visto, nunca he firmado nada, como le digo eso empieza a funcionar y se empieza en el camino a corregir y todo, pero así que ya este listo, algo, no, a no ser que no me haya dado cuenta.

5. ¿Ustedes se han dado cuenta que los programas, de pronto tienen problemas de exactitud, en cifras, en los resultados que arroja?
Hemos tenido varias veces.que no pasa, al mes siguiente las misma cifras, que aquí sumo y que aquí da un total y que no suma, pero se le informa a Fredy y él inmediatamente nos corrige.

6. ¿Me dice que lo procedimientos para comunicarse con el centro de informática son telefónicos…?
No, por lo regular uno habla con… cada uno maneja sus cosas… por lo regular es verbal, algunos escritos, pero por lo regular es comunicación directa ahí con Fredy.

7. ¿Entregan con puntualidad los trabajos por parte del Centro de Informática, son puntuales en las entregas?
No, no, siempre tenemos que estar pendientes, diciéndoles, insistiéndoles, requiriéndoles, siempre nos ocurre eso, uno ya se acostumbra.

8. ¿Tienen establecido algún horario o calendario fijo para la entrega de reportes, lo que tenga que ver con el Centro de Informática?
No, nosotros, o sea, los programas, que la contabilidad, que eso, ya esta, la contabilidad, el presupuesto, nosotros tenemos con esas entidades fechas, nosotros tenemos fechas y eso con tiempo hay que empezar a acosar para que en el momento este, o sea nosotros ya sabemos que hay que entregar por ejemplo la información exógena, por ejemplo dentro de tres meses entonces con tiempo vamos, empieza la funcionaria encargada con la existencia para poder cumplir nosotros.

9. ¿Se revisa por parte de la dirección, la información que va a ser ingresada a los diferentes programas o al programa de Contabilidad con los diferentes módulos por parte de la Dirección, antes de que lo ingresen los operarios?
Pero a ver, no se si ustedes han analizado como es la información, cada uno tiene sus funciones, entonces, cada uno digita su información, porque yo no podría estar ahí pendiente de cada uno, lo que mas se revisa son los resultados, digamos el Balance, los reportes, como va esa ejecución, los estado comparativos como dan, digamos que yo… ahora, la codificación si se revisa, se llega y se les dan las pautas que cómo deben codificar y todo esto, pero digamos que eso si resulta con muchos errores también y uno se da cuenta pues ya en lo balances y en los resultados – ¿Pero errores, por programación ? – Errores de código, de digitación o también que no era esta cuenta, que en lugar de llevarla a un ingreso era un depósito especial, bueno cuestiones así, pero eso mas que todo uno lo nota ya en los resultados, porque la niña que registra, que codifica, eso son cantidad de cuentas que le llegan y ella esta en eso, entonces yo no podría estar ahí pendiente que digito, que no digito, uno se da cuenta es en los resultados, si llego bien, en el análisis de costos, por ejemplo uno se da cuenta, hay muchos errores que tenemos que corregirlos, tenemos que ajustar a fin de año, cuando hacemos los análisis de costos o semestral o en el Balance, en el Balance mensual, pero mas que todo, mas que todo es en el Balance de fin de año, porque ahí se hacen los análisis de costos y eso si lo revisa es todo, entonces se hacen los ajuste aquí en el lugar.

10. ¿Para el ingreso a las instalaciones de esta dependencia, cuántas personas tienen llave de la puerta de acceso?
No, eso lo corrigieron, porque antes tenia llave todo el mundo, tengo yo – ¿Únicamente usted? – Si, pues yo le presto al funcionario que necesite quedarse.

11. ¿En la dependencia se ajustan a los horarios establecidos por la Universidad o sea de ocho a doce, de dos a seis o existe otro horario que maneje internamente la dependencia?
Pues nosotros, realmente esta dependencia como tiene tantos compromisos, hay que atender muchos informes y no solamente es Contabilidad, es presupuesto también, entonces por lo regular en el horario normal no alcanzamos, pues en épocas anteriores no quedábamos tranquilamente, siempre era pidiendo a Informática pues que los Sábados nos dejarán prendido el Sistema igual de seis a ocho, después hubo una orden de que todo mundo tenia que irse a las seis, entonces ya tuvimos que empezar a mandar cartas y a pedir que nos dejen trabajar, porque si no, no podemos cumplir, no alcanzamos en el tiempo, por mas que la gente permanece ahí, no se alcanza, no es que la gente salga y de pronto descuide su trabajo, no, sino que es mucho, la Contraloría, nos están pidiendo las dos contralorías, la nacional y la departamental y piden la misma información

desagregada en forma diferente, entonces de todas maneras hay que estar… ese es un trabajo bastante dispendioso

12. ¿Fuera de las jornadas laborales, quien autoriza la entrada a la dependencia, por ejemplo si un funcionario necesita trabajar en horas extras que no sean dentro del horario normal?

En este momento cada funcionario me dice, pero la apreciación la da el vicerrector o la.doctora encargada, el que este, la tienen que dar es ellos.

13. ¿Dentro de la dependencia de existe un control o hay un libre movimiento para los equipos o los equipos siempre tienen que estar en el mismo lugar y son lo funcionarios los que están rotando, como es este procedimiento?

Los equipos, prácticamente a cada uno se le asigna, pero por ejemplo hace poco tuvimos un problema de luz, se quemaron unas tarjetas, entonces se vio la forma de que… como le digo, de interconectare con otro, aquí tenemos a Oscar que es el ingeniero de Sistemas y el nos cuadra eso, empieza a sacarle la tarjeta al uno y ponérsela al otro, o sea, nos soluciona el problema de todas maneras, pero digamos entre los mismos equipos y no se acude a Informática y ellos nos prestan, que a veces dicen que les falta tal cosita, entonces vienen y nos la…o que les falta cable, que hagan esto, ellos solucionan ese problema – ¿Por parte del aula de Informática? – Del aula y de aquí de Oscar, Oscar nos apoya mucho en eso – ¿El es el Ingeniero de Sistemas de aquí? – Si, él nos ayuda mucho en todo esto de costos y todo esto de los equipos, especialmente que uno no sabe, uno llega y ya le prendió, pero entonces ya ellos miran y ya saben que es algo que tiene otro equipo y así los ponen a funcionar.

14. ¿Se prohíbe el uso de cigarrillo, comestibles bebidas, cerca a los computadores?
Si aquí las personas que fuman siempre se van a fumar a otra parte, van a la cafetería, aquí adentro no fuma nadie y comida pues no, rara vez, rara vez se come aquí adentro – ¿En la cafetería? – Si

15. ¿Se tiene una lista de personal encargado de los computadores, existe un solo responsable por cada equipo, genera responsabilidades de los equipos a cada persona?

Cada uno tiene que responder por lo que tiene, no solamente por el computador, por el teléfono, por todo, cada uno responde por lo suyo – ¿Pero la responsabilidad que se ha asignado es de forma verbal? – pues digamos en los inventarios que se firman vienen cada uno o sea en el inventario viene el nombre de cada funcionario, entonces ellos firman, entonces cuando traen los inventarios cada uno mire a ver si tiene todo o si le falta o si hay que descargar este, pues cada uno que este como pendiente de lo suyo.

16. ¿Se realiza un mantenimiento periódico de los computadores o no hay un mantenimiento?

No, si aquí incluso nosotros tenemos un equipo, como es que se llama… un equipo, que el equipo limpia y todo eso, Oscar se encarga de eso – ¿Y es periódico el mantenimiento o digamos es correctivo el mantenimiento, cuando se dañan los equipos, le hacen mantenimiento, se lo organiza? – Si por lo regular cuando se daña algo es que… ahí se entra a arreglar, pero digamos, así permanente, que sea una política de mantenimiento, no, aquí se limpia, se sopla, ahí hay un aparato que se compro aquí y se los mantiene soplando y todo eso – ¿Pero este es propio de la dependencia? – Si, este es de nosotros – ¿No tiene nada que ver ni con el centro ni con el aula de informática – No, a ellos se acude cuando se daña algo, pero que sea una cuestión periódica, que este pendientes que debía de ser, no, es lo mimo que uno espera a enfermares para ir al médico, aquí la ventaja que le digo es que tenemos a Oscar y cualquier cosita, ahí mismo nos soluciona, es por eso que no sentimos tanto, no sentimos tanto porque ya corre ahí donde los monitores o corre allá… y soluciona.

ANX26

ENTREVISTAS CON EL PERSONAL DEL CENTRO INFORMÁTICA

DE LA UNIVERSIDAD DE NARIÑO

CUESTIONARIO No. 1

CARGO: **JEFE DE SERVICIOS GENERALES**

Durante todo el día, él entra al las siete de la mañana y sale a las doce del día, entra a las dos de la tarde y sale a las seis de la tarde, físicamente bloque administrativo, en la noche viene la vigilancia, el señor que hace la vigilancia en la zona, toda el área administrativa, Biblioteca, Aula de Informática, Auditorio Luis Santander, los Bloques y el bloque administrativo, ese es la de la noche – ¿ellos tienen establecidos horas especificas para el recorrido? – No, ellos no tienen establecido recorrido específico, usted va a las seis de la tarde al bloque administrativo no, ellos revisan todo, se fijan si a las diez de la noche mas o menos, se termina el Servicio del Aula de Informática donde esta específicamente el Celador, pues se juntan los dos y hacen la ronda entre los dos – ¿por ejemplo en la noche cuando realizan la rondas, las hacen únicamente por el exterior del bloque administrativo o también ingresan – ellos también tienen llave y pueden ingresar si hay alguna anomalía dentro del bloque, tienen llave de la puerta principal del bloque y pueden entrar al bloque, no tienen llave de las oficinas ellos no tienen ninguna llave de las oficinas directamente ni del centro de informática, sino solo de la puerta principal de acceso para revisar por fuera o sea los corredores.

2. ¿Cuál es la capacitación que han recibido los vigilantes?
A los vigilantes se les dio Polígono para manejo de armas, con unos señores de una vigilancia privada que los llevaron al cuartel con unos señores del Batallón Boyacá, estuvieron en Chapalito, para manejo de armas.

3. ¿Cuáles son los horarios establecidos para realizar el aseo en el Centro de Informática?
Específicamente en el centro de Informática, si hay alguna cosa especial lo define el jefe del centro de informática que este ahí, él dice si se puede hacer en determinado momento o se deja de hacer en determinado momento por alguna cosa especial que tenga en el trabajo ellos, si no lo hacen antes de que lleguen los funcionarios para cuando ellos lleguen a trabajar a las ocho de la mañana, ya este listo y no tenga que hacer limpieza por encima de los trabajadores – ¿El

personal tiene llave del centro de Informática? El conserje asignado a esa área tiene llave para ingresar a hacer la limpieza– ¿el personal de aseo tiene algún tipo de capacitación o algo? – Si un ingeniero, se llama….

– ¿ ? – Por parte de Servicios Generales no, pero creo que por parte del director del Centro de Informática, si se dio el adiestramiento necesario para que tenga cuidado con los cables, para que… porque los equipos no los tocan ellos

ANX27

CARGO: **GERENTE DE EMPRESA DE SEGURIDAD VIP**

1. ¿Bajo que reglamentación se rigen los servicios de vigilancia y seguridad privada?
Los servicios de vigilancia y seguridad privada, se rigen, mediante el decreto 356 del 11 de febrero de 1994 por el cual el gobierno nacional establece una reglamentación para la Constitución y para el desarrollo de una empresa de vigilancia y seguridad privada y de los demás servicios de vigilancia y seguridad privada, porque también encontramos los departamentos de seguridad, las escuelas de capacitación y entrenamiento en vigilancia y seguridad privada, las cooperativas en vigilancia y seguridad privada, entonces el decreto 356, da directrices y rige a todos esos servicios de vigilancia y seguridad privada, mediante o por intervención de la superintendencia de vigilancia y seguridad privada.

2. ¿Todos los servicios de vigilancia y seguridad, deben regirse por la reglamentación mencionada anteriormente?

El gobierno nacional exige de que todos lo servicios de vigilancia y seguridad privada estén reglamentados por el decreto 356 y deben estar adscritos al Ministerio de defensa nacional y a la superintendencia de vigilancia y seguridad privada como organismo de control, inspección y vigilancia, sin embargo existen empresas, instituciones, conjuntos residenciales, barrios, almacenes, que tienen el servicio de vigilancia y seguridad, pero en forma pirata o sea que no están autorizados ni por el Ministerio de Defensa nacional, ni por la superintendencia de vigilancia y seguridad privada todo servicio de vigilancia y seguridad tiene que estar regido por el Ministerio de Defensa Nacional y por la Superintendencia de vigilancia y seguridad privada, quiénes son los encargados de prestar este servicio, las empresas de vigilancia y seguridad privada, ninguna persona natural, ni ninguna persona jurídica puede por su cuenta contratar personal para que desempeñe en funciones de vigilancia y de seguridad por ejemplo en los conjuntos residenciales le dicen que es el portero, pero ese portero esta prestando un servicio de vigilancia y seguridad porque el solo hecho de abrir y cerrar la puerta ya es seguridad, el solo hecho de requisar un bolso es seguridad y únicamente pueden hacerlo las personas entrenadas y capacitadas para eso y que estén autorizadas por el gobierno nacional para prestar este servicio.

3. ¿Existen parámetros para establecer el número de vigilantes necesarios de acuerdo al espacio?
Si existen unos parámetros, un vigilante puede abarcar una visual de cincuenta metro o sea media cuadra, cuando ya se pasa su visual de cincuenta metros ya no puedo prestar un servicio optimo, ahora nosotros tenemos en cuenta para la asignación del numero de vigilantes esta directiva o este parámetro, entonces si la extensión a vigilar a custodiar es muy grande, si se hace necesario que se instale uno o dos vigilantes, o sea, si se pasa ya de cincuenta metros, toca utilizar otro vigilante, por qué, porque la visual incluso de él, después de cincuenta metros ya no es optima, entonces no se va a dar cuenta que están haciendo a cincuenta metros de distancia.

4. ¿En un edificio, cómo se realiza este procedimiento, es de acuerdo a los pisos o de que manera?
En un edifico nosotros tenemos que analizar, digamos las entradas, cuántas entradas tiene el edificio, si tiene parqueadero, si tiene ascensor, si tiene salida de emergencia y además nosotros establecemos el valor de los equipos, a custodiar, el valor de la información porque digamos, si es un edificio simplemente que esta deshabitado, que todavía no esta en operación entonces tranquilamente se puede colocar un vigilante en la entrada, no más, pero si ya es un edifico en el cual funcionen oficinas que tiene unos equipos muy costosos, entonces ya se recomienda que en un piso determinado tiene que haber un vigilante, aparte del de la entrada por qué, porque en ese edificio se encuentran veinte, treinta computadores o porque en ese edificio funciona la parte contable y administrativa y además también se guarda dinero o también se puede ver que en determinado piso se encuentra los funcionarios en la parte directiva mas fuerte de ese edificio o

personalidades como ministros, como senadores, rectores, entonces, hay también amerita colocarles otro vigilante entonces digamos ya ese edificio tendría un vigilante en la portería, tendría otro vigilante en el parqueadero y tendría un vigilante en el piso de la administración y otro vigilante en el piso donde operan los funcionario mas destacados o las personalidades que pueden ser victimas de un secuestro.

5. ¿Respecto al personal de vigilancia, qué estudio e le realiza a la hoja de vida de una persona que desea ingresar a una empresa de vigilancia y seguridad privada?
La Superintendencia de vigilancia y seguridad privada ha querido que el personal que trabaja en vigilancia y seguridad privada sea idóneo en el tema y por eso crearon las escuelas de capacitación en vigilancia y seguridad privada ya que en tiempos pasados, para que una persona trabaje en vigilancia y seguridad privada, el único requisito era que él haya prestado el servicio militar obligatorio y tenga una tarjeta de conducta excelente, entonces ese era el requisito primordial, usted prestó servicio militar, si, usted tiene tarjeta de conducta excelente, si, entonces puede trabajar en vigilancia y seguridad privada, sin embargo se le estaba negando el derecho a trabajo al personal que no había ido a prestar servicio militar por x o y razón, entonces ese personaje se quedaba por fuera de las empresas de vigilancia y seguridad privada, entonces a raíz de eso, se crearon la escuelas de capacitación y entrenamiento en vigilancia y seguridad privada donde la persona que de trabajar en seguridad, tiene que efectuar unos cursos, esos curso hoy en día son, el curso de introducción a la vigilancia y seguridad privada el curso básico de vigilancia y el curso avanzado de vigilancia y también hay una especialización y esas especializaciones son en escoltas, en supervisión, en escolta personalidades, escolta mercancías, seguridad bancaria, seguridad hotelera, seguridad educativa, seguridad residencial, seguridad hospitalaria, entonces este joven que desea ingresar a una empresa de vigilancia y seguridad privada tiene que venir con el curso de introducción y el curso básico, no nos importa si él es reservista de primera clase o de segunda clase, lo que nos importa es que tenga definida su situación militar, entonces llega a la empresa con su hoja de vida y en la hoja de vida reza el curso de introducción a la vigilancia y seguridad privada y el curo básico de vigilancia, entonces nosotros, le recibimos la hoja de vida en el momento de que ya se lo incorpora, digamos para trabajar porque el requisito básico para presentar la hoja de vida es tener el curso de introducción y el básico de vigilancia, cuando ya se lo llama a él para trabajar, entonces se le efectúa unas pruebas psicotécnicas, en las cuales se ve la habilidad mental, la personalidad, la formación familiar, la visión que él tiene hacia el futuro, la seguridad personal y también se le hace una visita domiciliaria, si el joven pasa la prueba psicotécnica y también pasa la visita domiciliaria, entonces lógicamente se lo incorpora a la empresa.

6. ¿Qué capacitación recibe el personal de vigilancia?
La Capacitación que recibe el personal de vigilancia como lo dije anteriormente son los cursos de Introducción, básico, avanzado y la especialización, qué miran el

curso de introducción, en el curso de introducción miran lo que es normatividad legal, miran primeros auxilios, miran ética y profesionalismo y un ejercicio practico de tiro. En el curso avanzado ya miran Psicología, Derecho, se hace otro ejercicio práctico de tiro con otra clase de armamento, o sea en introducción pueden disparar revólver y en el curo básico ya disparan pistola y el curso avanzado disparan ya escopeta, entonces a medida de que ellos van haciendo sus respectivos niveles de capacitación, van avanzando más y van ahondando mas los temas en que se deben capacitar.

7. ¿Cómo se realiza el control de visitas en las instituciones, tanto para personas como para vehículos?
Eso depende del estudio de seguridad física que se haga a la institución y de las necesidades que tenga esa institución, entonces digamos que el control de visitas en un centro educativo, entonces el procedimiento que se debe hacer es primero el saludo, bueno días, buenas tardes, buenas noches en qué lo podemos servir, luego se le pide un documento al persona que va a ingresar un documento que no sea la cédula, después de que esa persona nos entrega el documento, se le entrega una escarapela, después de entregarle la escarapela, se le hace una pequeña requisa y se le indica donde queda la instalación o donde se encuentra la persona a quien el esta necesitando y va a visitar, también se suele llenar una ficha de visita, en esa ficha de visita o en esa hoja, se llenan los datos de la persona, el nombre completo, el número de la cédula, a qué persona va a visitar, en qué dependencia se encuentra e incluso se le hace firmar al visitante y luego cuando el señor salga, el visitante salga tiene que traer la hoja firmada por la persona que fue a visitar, o sea eso depende de las necesidades que tiene la institución como tal, entonces hay entidades donde si toca hacer una requisa demasiadamente minuciosa como por decir algo hasta hacer desnudar a una persona y hay otras entidades donde simplemente se le requisa el bolso, entonces depende de las necesidades y del riesgo que tenga esa empresa, que tenga esa institución, que tengan esas personas.

8. ¿Cómo se realiza el control del personal perteneciente a la Institución?
El control de personal de la institución, se realiza mediante el carnet de la institución o sea es imagen corporativa también de que todos los empleados de esa institución porten una escarapela o un carnet, entonces, ese carnet lo deben presentar a la entrada al vigilante, entonces el verifica los dato y verifica la fotografía y lo deja seguir, ese sería un mecanismo, otro mecanismo es que en la portería también estén los nombre y las cédulas del personal que trabaja en la institución y es una planilla diaria donde se va chuleando al funcionario, el día, el me, el año y la hora de ingreso, entonces podíamos utilizar cualquiera de esos dos, ahora también hay un mecanismo y tecnología mas avanzada para el control de accesos, entonces también depende de la capacidad económica que tenga esa empresa, esa institución para incrementar un mecanismo mas adecuado de control de accesos, pero si no se cuenta con esos recursos, simplemente pues se carnetiza a todo el personal de la institución o se deja una lista de todo el personal

de la institución en la portería, el vigilante se encarga de verificar los nombres o verificar ese carnet

9. ¿Igualmente, cómo se controla la entrada y salida de equipos de computo o telecomunicaciones del establecimiento?

.El gerente de la empresa de vigilancia y seguridad privada o el jefe operativo de la empresa de vigilancia y seguridad privada se reúne con el gerente o con el director o con el rector o con el encargado de la empresa la cual se va a custodiar o a la cual se le va a prestar el servicio de vigilancia y seguridad privada y dialogan de acuerdo a qué necesidades tiene, a que falencias y a que fortalezas, entonces ya después de esa conversación que tenga tanto el gerente de la empresa como el gerente de la empresa de vigilancia y seguridad privada con el gerente de esa institución, entonces optan unas medias aconsejables y que se puedan poner en practica en esa institución, por ejemplo, para la entrada y salida de todo equipo, el único que autoriza, digamos la salida, es el rector o es el gerente, mediante una ficha o una hojita donde va especificado, la persona que va a sacar ese elemento, la característica de ese elemento, el número de control interno de ese elemento, el número de serie y lógicamente la firma del funcionario o el rector o de la persona que en esa empresa este autorizada para que se saquen lo equipos o cualquier clase de elementos, es mas también debe en la portería donde se encuentra el vigilante debe haber una hoja donde se encuentran las firmas de cada uno de los funcionarios, por qué, porque de pronto cualquier persona llega y hace una firma en esa hoja, la fotocopia y ahí le llena todos eso datos y hace una firma, entonces el vigilante mira esa firma y va a verificarla con el registro de firmas que tiene allá, entonces la mira y dice no que pena esta firma no es del rector, él es el único autorizado para sacar elementos de cualquier clase acá en la universidad yo no lo puedo dejar salir con este elemento y de inmediato coge ese equipo y lo deja en la oficina o en la dependencia de vigilancia y luego llama al rector a informarle que querían sacar un equipo, o sea detiene el equipo y detiene a la persona que iba a sacar ese equipo, esto cuando se tratan de universidades, hospitales y de fábricas donde se manejan equipos muy cotosos y hay cantidad, volumen de equipo, es muy necesario, tanto el control interno y el control de inventarios que debe hacer esa empresa porque todos los elemento de una empresa tienen que esta inventariados, mediante un número, puede ser alfanumérico o simplemente puede ser numérico, entonces el vigilante con la hojita se encarga de verificar el número de serie que tiene el equipo y el número de serie que viene en la hoja y con la firma puede ver si esta autorizado para sacarlo o no esta autorizado, esto tiene que ser en original y copia y el original lo dejan en la portería y la copia la lleva la persona que va a sacar el equipo, cuando vuelva el equipo, vuelve con la boletica y se verifica también el estado y demás y se lo deja otra vez seguir, ese sería un procedimiento que se podría optar, pero es necesario el control de los inventarios.

10. ¿Qué equipos o procedimientos establecen para el proceso de rondas de vigilantes?
Nosotros en las empresas de vigilancia y seguridad privada tenemos unos relojes de marcación, los cuales constan de unas llaves, esas llaves están ubicadas en sitios estratégicos de la empresa cada cincuenta metros se coloca una llave y el vigilante carga el reloj con él, entonces cuando el pasa por determinado punto mete la llave en el reloj de marcación y esto queda guardado en una cinta que tiene el reloj y luego cuando se moviliza al otro punto, allá hay otra llave la mete en el reloj y también queda marcada en la cinta, al otro día el supervisos revisa esa cinta y se da cuenta si el ha hecho la ronda, por qué, porque ahí queda en la cinta el registro de la llave, cada llave tiene una numeración y la hora y el día, entonces, se puede controlar de que el vigilante esté haciendo la ronda, porque necesariamente tiene que pasar por cada uno de lo puntos donde esta la llave – ¿Más o menos que periodos de tiempo se estiman? – Depende del espacio que tenga que cubrir, entonces en el estudio de seguridad, se toman los tiempos, primero se establecen, cuáles son los puntos más críticos de la empresa o de la institución que ameritan que el vigilante este haciendo rondas, entonces ya establecidos los puntos mas críticos, los que requieren mas seguridad, donde se encuentran los equipos mas cotosos, donde se encuentran la información mas clasificada, entonces nosotros hacemos ese análisis y allí instalamos una llave y de ahí desde ese punto donde hemos instalado la llave para el reloj de marcación tomamos tiempo hacia el otro punto, para qué, para que el vigilante no se vaya tan despacio o para que el vigilante vaya bien despacio, entonces, tomamos digamos el tiempo de un punto al otro punto, pero es de acuerdo a esa necesidad, esa necesidad de protección que haya porque si solo tenemos un auditorio donde solo hay sillas, no amerita tanta seguridad, ni tanta ronda como un bloque donde se encuentren cincuenta, sesenta computadores, entonces, eso nosotros lo establecemos, decimos a este sitio, a este bloque toca hacerle tres supervisiones o sea el vigilante tiene que marcar tres veces en el lapso de… tiene que marcar tres veces en la llave, en el reloj de marcación en el lapso de media hora o en el lapso de una hora, entonces de acuerdo al valor de los equipos a custodiar o la importancia de la información que haya en determinado lugar, en determinado bloque.

11. ¿Frente a posibles ingresos forzosos qué medidas debe tomar el personal de vigilancia?
El personal de vigilancia cuando suceden estos acontecimientos, el ultimo recurso, el ultimo recurso que debe utilizar el vigilante es el arma, cuando se le entrega al vigilante el arma de dotación se le dice vea joven, este es el último recurso que usted debe utilizar, el último, ya cuando se hayan agotado muchos recursos, entonces ya usted utiliza el arma, ellos en los cursos de entrenamiento que ya habíamos mencionado anteriormente, tienen defensa personal, en estas clases de defensa personal les enseñan llaves para la inmovilización de una persona, entonces si ya una persona se

pone agresiva y quiere entrar a al fuerza, entonces el vigilante le aplica una llave, la cual lo inmoviliza, hasta que la persona se calme y ya calmada, se le dice que quiere, en que lo podemos servir, entonces ese mecanismo utilizamos para ese personal que se porta pues agresivo, grosero.

12. ¿Cuándo se trata de sabotaje, por ejemplo, cuando se utilizan papas bombas, qué procedimiento realiza el personal de vigilancia?

Cuando hay manifestaciones de estudiantes en las cuales utilizan las papas explosivas y demás el procedimiento que se tiene previsto es el de cerrar puertas y ventanas o sea asegurar las dependencias y asegurar las porterías para que esta gente no pueda efectuar el ingreso e inmediatamente nos comunicamos por línea directa, radial con la policía nacional, para que por favor nos envíen el grupo antimotines, es mas cuando suceden esta turbas y cuando hay esas manifestaciones, nosotros optamos hasta por recoger el armamento o por guardar este armamento, por qué, porque el vigilante no puede hacer el frente a unas cinco, diez personas que se le abalancen ante él con el arma de dotación, entonces estimamos en cada portería, hay un locker donde ellos pueden guardar al arma, para que primero no se la quiten y con la misma lo pueden agredir a él o con esa arma pueden agredir a otras personas, entonces ese es el procedimiento, sellar absolutamente todo, echar lleva, cerrar y llamar a la policía para que envíen el grupo antimotines.

13. ¿Qué aspectos se debe considerar para un estudio de seguridad?

Un estudio de seguridad es muy complejo son más o menos ciento cincuenta o doscientos puntos que se deben aplicar para el estudio de seguridad, ahora eso también depende de la instalaciones a que se les vaya a efectuar el estudio de seguridad, porque hay entidades que requieren una seguridad física, mas rigurosa que otras, pero podemos mencionar unos aspectos, por ejemplo, la seguridad básica, primero debemos definir los términos de uso más frecuente, la amenaza, el nivel de riesgo, el plan de seguridad, prevención de perdidas, control de accesos, grado de autoridad del personal de seguridad, actividades claves e importantes, líneas de defensa o de seguridad, luego tenemos el punto de seguridad aplicada, en la capacitación, aspectos legales, redacción de informes, observación y descripción, requisas, patrullaje, primeros auxilios, manejo de personas perturbadas, otro punto tenemos la seguridad técnica, armas y municiones, comunicaciones, emergencias, sabotajes, incendios, evacuaciones y control del transito, también debemos tener en cuenta la seguridad personal y dentro de esa seguridad personal tenemos que ver la amenaza y el riesgo, el secuestro, amenazas de riesgo, peligro, evacuación de la amenaza, tenemos que tener en cuenta también el manejo de los mensajes, manejo de los mensajes telefónicos y escritos, características de la voz, ruidos de fondo mas comunes, los

mensajes escritos y las cartas, las relaciones con las autoridades, normas de prevención, normas de seguridad preventiva en cuanto a la sala de seguridad, ser lógico también, esos serian uno aspectos que nosotros debemos o tenemos y hacemos en un estudio de seguridad, pero como le digo el estudio de seguridad lo hacemos de acuerdo al factor de riesgo y de acuerdo al peligro en que se encuentre esa dependencia, entonces nosotros miramos la ubicación de esa empresa, miramos también el vecindario todos estos son factores de riesgo, por ejemplo, si nosotros vamos a hacerle el estudio de seguridad a una cárcel, entonces tenemos que tener una medidas extremas en seguridad y si nosotros le vamos a hacer el estudio de seguridad a un convento, entonces, lógicamente no se va a tener las medidas de seguridad, ni se va ha hacer el estudio de seguridad como se hizo en la cárcel, ahora que si el convento se encuentra dentro de la cárcel, ya es otra cosa.

14. ¿Qué dispositivos de seguridad se recomiendan para establecer un sistema de seguridad óptimo?
Para establecer un sistema de seguridad óptimo, estilo embajada de los Estados Unidos acá en Colombia, nosotros tenemos que tener en cuenta, primero, la seguridad física, o sea seguridad física y de instalaciones, tenemos que tener en cuenta la seguridad personal o sea la seguridad para las personas que trabajan en esa dependencia, también tenemos que tener en cuenta la seguridad técnica o sea que aquí ya hay la implementación de circuito cerrado de televisión, control de accesos biométricos, alarmas, inspecciones de seguridad, monitoreo y seguridad electrónica, o sea prácticamente digamos hacer un bunker, entonces, primero la seguridad física de las instalaciones, luego la seguridad del personal y luego la implantación de medios de seguridad electrónica, entonces eso sería lo óptimo en seguridad, dentro de esos medios, como ya mencionaba, circuito cerrado de televisión, control de acceso magnéticos, alarmas en la dependencias, entonces hay ya queda una entidad muy bien protegida o sea dónde recomendamos nosotros que se colocan… a parte de la seguridad física, o sea a parte de que se tenga un vigilante allí, recomendamos colocar una alarma, en aulas, por ejemplo, de informática, en las oficinas de contabilidad, entonces decimos, bueno si se colocó una seguridad física, hay esta el vigilante, pero es necesario que se coloque una alarma en esta dependencia, porqué, porque ahí hay cincuenta computadores, entonces es bueno colocar esa alarma.

15. ¿En lo que se refiere al control de accesos, qué medidas de seguridad se tienen para el ingreso de vehículos?
Hoy en día de acuerdo a la situación de riesgo y de peligro que se encuentra nuestra amada Colombia y de los medios que esta utilizando lo grupos terroristas, uno de esos medios son los famosos carros bomba, entonces los vigilantes los vigilantes tienen una capacitación especial para eso, primero cuentan con un espejo de piso que se utiliza para mirar el vehículo por debajo, o sea qué examinan ellos en la parte de abajo del vehículo o sea en el chasis, que no hayan elementos adheridos al chasis, que no hayan cables por debajo del vehículo o sea

lo grupos terroristas utilizan lo vehículos para la instalación de artefactos explosivos, entonces el vigilante tiene que ver si ese vehículo tiene mucho peso en la parte de atrás o sea en el baúl o si todo el carro esta asentado o sea en las cuatro llantas, porqué, porque si va una sola persona, porque el carro esta tan sentado, entonces quiere decir que lleva explosivo, el tablero también, o sea la parte de adelante, que no hayan cables volando, porqué, por que en los vehículos todo esta debidamente diseñado, entonces si ya hay un cable suelto, entonces eso ya es un indicio de que puede haber un artefacto explosivo, qué otra parte del vehículo se debe revisar, el baúl, el motor, los guardabarros y la parte de abajo del vehículo, eso en cuanto a un carro bomba, por decir algo que nos vayan a meter un carro bomba, pero el procedimiento de rutina con los vehículos es lógicamente requisarlos al interior del vehículo, o sea la persona tiene que bajar del vehículo para que el vigilante revise el interior del vehículo a ver si no saca un equipo o cualquier elemento de propiedad de esa empresa o esa institución, de igual forma el baúl y lo vehículos que son del común de esta empresa, deben tener una calcomanía y en la entrada del parqueadero se verifica las placas del vehículo y el propietario de ese vehículo, o sea que si otra persona va a sacar ese vehículo, tiene que ser con autorización del propietario, firmado, porqué, por que no puede llegar que mi amigo me presto el carro y yo lo voy a sacar, no, tiene que ser con una autorización del dueño de ese vehículo y cómo sabemos que es el dueño, lógicamente ahí en la portería esta registrado el nombre del dueño del vehículo, las placas, todos lo datos que tienen que ver con el dueño del vehículo y con el automotor, entonces hay controlamos la entrada y salida de vehículos, hoy en día es muy frecuente lo de los carros bomba y el robo de vehículos dentro de las instalaciones, entonces, eso es fundamental.

.