UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING

ANÁLISIS Y DISEÑO DE LA SEGURIDAD DE SOFTWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

FÁTIMA DEL ROCÍO CARVAJAL QUIMIZ

TUTOR: ING. FRANCISCO PALACIOS O.

GUAYAQUIL – ECUADOR

2011

Guayaquil, Septiembre del 2011

APROBACION DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "Análisis y Diseño de la seguridad de software del Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking" elaborado por la Srta. Fátima del Rocío Carvajal Quimiz, egresada de la Carrera de Ingeniería en Sistemas Computacionales, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

……...…….
ING. FRANCISCO PALACIOS O.
TUTOR

DEDICATORIA

A Dios porque siempre estuvo a mi lado cuidándome y guiándome en cada paso que doy, por darme la fortaleza para continuar.

A mis padres Paula Quimiz y Carlos Carvajal por brindarme su apoyo incondicional, su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, quienes depositaron su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad, a quienes les debo la vida y hecho de ser quien soy.

A mi hijo Sebastián Paúl el ser más especial que bajo del cielo para llenar de alegría mi vida, eres mi inspiración y fortaleza el motor que me obliga a funcionar para ser mejor cada día, a él mi esperanza, mi alegría, mi vida, y la culminación de este trabajo y lo que representa.

A mis hermanos Yessica, John, Andrés y Karen quienes siempre creyeron en mí, lo amo.

AGRADECIMIENTO

Al Ing. Francisco Palacios por dedicar su tiempo y paciencia de manera desinteresada, por compartir sus conocimientos en el desarrollo de este proyecto.

Del mismo modo quisiera expresar mi agradecimiento a todos quienes estuvieron vinculados de alguna manera a este proyecto, al personal del Departamento Técnico Informático de la Carrera de Ingeniería en Sistema Computacionales quienes me proporcionaron la información necesaria para completar esta investigación.

TRIBUNAL DE GRADO

DECANO DE LA FACULTAD
CIENCIAS MATEMATICAS Y FISICAS

DIRECTOR

TUTOR

PROFESOR DEL ÁREA - TRIBUNAL

PROFESOR DEL ÁREA - TRIBUNAL

SECRETARIO

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING

ANÁLISIS Y DISEÑO DE LA SEGURIDAD DE SOFTWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING

Proyecto de trabajo de grado que se presenta como requisito para optar por el título de INGENIERO EN SISTEMAS COMPUTACIONALES

Autora: Fátima del Rocío Carvajal Quimiz
C.I.:0921243069
Tutor: Ing. Francisco Palacios O.

Guayaquil, Septiembre del 2011

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del Segundo Curso de Fin de Carrera, nombrado por el Departamento de Graduación y la Dirección de la Carrera de Ingeniería en Sistemas Computacionales de La Universidad de Guayaquil,

CERTIFICO:

Que he analizado el Proyecto de Grado presentado por la egresada Fátima del Rocío Carvajal Quimiz, como requisito previo para optar por el título de Ingeniero cuyo problema es:

ANÁLISIS Y DISEÑO DE LA SEGURIDAD DE SOFTWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING

Considero aprobado el trabajo en su totalidad.
Presentado por:

_____
CARVAJAL QUIMIZ FATIMA DEL ROCIO
092124306-9

Tutor: _____
Ing. Francisco Palacios O.

Guayaquil, Septiembre del 2011

INDICE GENERAL

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

Debido al crecimiento de las redes informáticas la seguridad de los sistemas se ve altamente debilitada y al tratar este tema hay que tomar en cuenta la integridad de los datos, es decir, si no existe una barrera cien por ciento segura que nos pueda garantizar la privacidad de nuestra información debemos tener presente que esta puede ser violada y modificada de manera perjudicial para nuestra organización.

En la actualidad podemos acceder a cualquier tipo de información a través de la red internet. Sin embargo, esto plantea algunos inconvenientes prácticos. Las redes y sistemas informáticos se han convertido en un nuevo espacio para el delito: interceptar comunicaciones electrónicas entre dos personas, introducirse en los sistemas informáticos de empresas, divulgar y transferir ciertos datos industriales, dañar, cambiar o alterar datos, programas o documentos electrónicos son los principales casos de estafas en la red.

Actualmente existen dispositivos extraíbles que al ser conectado en el computador pueden guardar contraseñas, datos y demás sin que nos percatemos de lo que ocurre, es decir que podemos tener flujo de información, manipulación de la base de datos, alteración de nuestro sistema informático, etc. Sin embargo a pesar de las múltiples maneras de acceder a una red aún nos vemos envueltos en situaciones poco seguras

para protegerla tomando en cuenta que se deben resguardar elementos como el software y datos, de todo intento de acceso no autorizado desde el exterior y contra cierto ataques desde el interior que pueden prevenirse.

La seguridad informática es de tal importancia que debería considerarse como un método fundamental y básico para cualquier organización, sin embargo aún se considera como un procedimiento no tan importante o no tan necesario, hoy en día la mayoría de las organizaciones tienen como prioridad comercializar sus productos e incrementar sus utilidades y le restan importancia a los niveles de protección o a los riesgos que puede tener su Data Center.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

En la actualidad hablar de Seguridad Informática en nuestra institución es tratar un tema no muy relevante, por tal motivo el Administrador del Departamento Técnico Informático debe decidir de acuerdo a las jerarquías quienes tendrán acceso a todo tipo de información y quienes no lo tendrán dependiendo del área en que desempeñan sus labores, de esta manera se evitará que se filtre información o pueda ser utilizada de manera poco favorable para nuestra organización, debemos llevar sistemas de detección de intrusos, no dejemos accesos a los intrusos por la falta de conocimientos sobre seguridad informática.

Por este motivo debemos tener claramente definidas, documentadas y principalmente ejecutadas las normas, reglamentos y protocolos de seguridad porque estas nos ayudaran a contrarrestar las posibles infiltraciones a nuestra red, y utilizar de forma correcta los recursos que la institución pone en juego para disponer de un eficiente y eficaz Sistema de Información.

Un Data Center debe constar con el software necesario para cumplir con todas las funciones que le corresponden pero una de las principales causas que nos lleva a limitarlos en la seguridad lógica es el factor económico ya que no es suficiente realizar estudios e investigaciones sin implementar los resultados del mismo.

Debemos mejorar la calidad de la seguridad del software, crear conciencia acerca de los riesgos a los que estamos expuestos si no ponemos en práctica todas las normas que nos ayuden con la seguridad del Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas y NetWorking.

EVALUACIÓN DEL PROBLEMA

Es una realidad que El Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales no consta con las normas de seguridad preventivas y operativas, con apoyo de procedimientos, programas, sistemas, y equipos de seguridad y protección, orientados a neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia, que afecten y lesionen a las personas o los bienes de ésta.

Por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las Violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas. El

resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles de dólares.

Por las razones citadas anteriormente debemos tener presente las amenazas a las que estamos expuestos en el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking si carecemos de protección de software y dejamos que nuestro sistema sea vulnerable y accesible por falta de conocimientos de seguridad informática.

El presente proyecto es realizado en la Universidad de Guayaquil – Facultad de Ciencias Matemáticas y Físicas – Carrera de Ingeniería en Sistemas Computacionales y NetWorking ubicada en la Ciudad de Guayaquil – Ecuador.

OBJETIVO GENERAL

Realizar un análisis que permita identificar como nuestro sistema es afectado por la falta de seguridad lógica para así realizar un diseño que cubra las vulnerabilidades que tiene el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking.

OBJETIVOS ESPECÍFICOS

- ✓ Levantar información que permita conocer detalladamente la parte lógica que se maneja dentro del Departamento Técnico Informático de la Carrera Ingeniería en Sistemas Computacionales y NetWorking.
- ✓ Revisar las políticas, normas y protocolos de seguridad informática en software del Departamento Técnico Informático de la Carrera Ingeniería en Sistemas Computacionales y NetWorking.
- ✓ Evaluar los puntos vulnerables que llegase a tener la seguridad informática en software del departamento Técnico Informático de la Carrera de Ingeniería en Sistema Computacionales y NetWorking.
- ✓ Realizar el diseño de las soluciones a las anomalías lógicas encontradas en la seguridad informática en software del departamento Técnico Informático de la Carrera de Ingeniería en Sistema Computacionales y NetWorking.

JUSTIFICACIÓN E IMPORTANCIA

Este proyecto es realizado con la finalidad de dar a conocer la importancia de la seguridad informática en software y los riegos a los que somos vulnerables en el Departamento Técnico Informático de Carrera de Ingeniería Computacionales y NetWorking ya que este no consta con la información ni los procedimientos necesarios para desempeñar sus funciones de forma óptima.

Existen vulnerabilidades a los que estamos expuestos como virus, gusanos, códigos maliciosos, etc. y con el avance de la tecnología han incrementado las maneras de filtrarnos a otra red ahora también debemos estar atentos al "hackeo", vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Es importante decidir cuáles serán nuestras políticas de seguridad entre las cuales se debe tomar en cuenta el monitoreo de la red, enlaces de telecomunicaciones, respaldo de datos y establecer niveles de protección de recursos, de esta forma garantizaremos la protección de nuestro software.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

Muchas organizaciones a nivel mundial como El Pentágono, UNICEF, La ONU, etc. han sido víctimas de ataques por parte de los llamados "Hackers" que tienen muchos conocimientos y también una gran capacidad para resolver los obstáculos que se les presentan, estos no necesitan la última tecnología para intervenir nuestra red, solo basta computadora y un modem que les ayude a la conexión, sin mencionar que existen miles de páginas web en las que los piratas informáticos pueden encontrar todo tipo de trucos y herramientas que les facilita cada vez más el descifrado de claves para tener accesos a la información indebida.

Cuando nos conectamos a la Gran Red Internet debemos tener en cuenta la cantidad de amenazas a los que estamos expuestos, virus y spam solo son los principales peligros que debemos contrarrestar día a día para que nuestro sistema no sea afectado de manera perjudicial.

La Seguridad de la Información se ha convertido en un área clave en el mundo interconectado de hoy. Día a día, en los principales medios de comunicación se

repiten los ataques de virus, hackers y otros peligros tecnológicos. Desde el ámbito corporativo y gubernamental, la búsqueda de profesionales en Seguridad Informática se ha duplicado y la tendencia sigue en aumento.

FUNDAMENTACIÓN TEÓRICA

La seguridad informática es el área que se enfoca en la protección de la infraestructura y la información computacional. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad de la información es una subárea de la seguridad informática que se enfoca exclusivamente en la protección de la información, lo que comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Objetivos de la seguridad informática

La seguridad informática está concebida para proteger los activos informáticos de la empresa, entre los que se encuentran:

La información: Hoy en día la información se ha convertido en uno de los activos más importantes y valiosos dentro de una organización. La seguridad informática debe velar por que ésta sea administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o

que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La infraestructura computacional: Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de contingencia que permitan su rápida reposición. También debe asegurar que las redes y toda la infraestructura funcionen correctamente; para ello se deben realizar mantenciones periódicas para detectar posibles fallas en la misma. Por último, la seguridad informática debe asegurar planes de contingencia en caso de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios: Son las personas que utilizan la estructura tecnológica, de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad

informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

El usuario: Causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

Programas maliciosos: Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en el computador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un spyware.

Un intruso: Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).

Un siniestro (robo, incendio, inundación): Una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

Tipos de amenaza

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Secutiry Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

-Los usuarios conocen la red y saben cómo es su funcionamiento.

-Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

-Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

Amenazas externas: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

VIRUS INFORMÁTICO

Un **virus informático** es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su

ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Tipos de Virus

Los virus se pueden clasificar de la siguiente forma:

Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Virus de boot o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el ordenador con un disquete desconocido en la disquetera.

Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

Virus de macro

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc. Las macros son micro-programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Virus cifrados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

Virus polimórficos

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus de Fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema.Los virus que atacan a este elemento son especialmente peligrosos, ya que

impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Debemos tener en cuenta los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

Identificación y Autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.

- Algo que la persona **posee:** por ejemplo una tarjeta magnética.
- Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de **hacer:** por ejemplo los patrones de escritura.

Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- ✓ **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- ✓ **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- ✓ **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- ✓ **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- ✓ **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- ✓ **Búsqueda:** permite listar los archivos de un directorio determinado.
- ✓ Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

CONTROL DE ACCESO INTERNO

Palabras Claves (Passwords)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

Sincronización de password:

Consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario.

Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes password tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de password entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

Caducidad y control

Este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

Listas de Control de Accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Límites sobre la Interface de Usuario

Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interface de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

Etiquetas de Seguridad

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

CONTROL DE ACCESO EXTERNO

Dispositivos de Control de Puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

Firewalls o Puertas de Seguridad

Un **muro de fuego** (***firewall*** en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos una tercera red, llamada *Zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Ilustración 1: Esquema de una red de computadoras que utiliza un Cortafuegos

Elaboración: www.wikipedia.com

Fuente: www.wikipedia.com

Tipos de cortafuegos

Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino, etc. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección

MAC. Este es uno de los principales tipos de cortafuegos. Se considera bastante eficaz y transparente pero difícil de configurar.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por

Ventajas de un cortafuegos

Establece perímetros confiables.

Protege de intrusiones.- El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

Protección de información privada.- Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.

Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un cortafuegos

Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

- El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- El cortafuegos no puede proteger contra los ataques de ingeniería social.
- El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

Políticas del cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará

ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

PROXY

En el contexto de las redes informáticas, el término **proxy** hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Ilustración 2: Esquema de un servidor proxy

Elaboración: http://saurabarbara.blogspot.com/2010/06/glosario-de-guerreros-de-la-red.html

Fuente: http://saurabarbara.blogspot.com/2010/06/glosario-de-guerreros-de-la-red.html

La palabra **proxy** se usa en situaciones en donde tiene sentido un *intermediario*. El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino. De ellos, el más famoso es el **servidor proxy web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.

También existen proxies para otros protocolos, como el **proxy de FTP**.
El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Un componente hardware también puede actuar como intermediario para otros.
Fuera de la informática, un *proxy* puede ser una persona autorizada para actuar en **representación** de otra persona; por ejemplo, alguien a quien le han delegado el derecho a voto.

Una *guerra proxy* es una en la que las dos potencias usan a terceros para el enfrentamiento directo.

Como se ve, **proxy** tiene un significado muy general, aunque siempre es sinónimo de **intermediario**. También se puede traducir por **delegado** o **apoderado** (el que tiene el poder).

Ventajas

En general (no sólo en informática), los proxies hacen posibles varias cosas nuevas:

- **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- **Abuso**. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- **Carga**. Un proxy ha de hacer el trabajo de *muchos* usuarios.
- **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- **Incoherencia**. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.
- **Irregularidad**. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

Funcionamiento

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

PORTAL CAUTIVO

Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. A veces esto se hace para pedir una autenticaciónválida, o para informar de las condiciones de uso de un servicio wireless (que es donde más se encuentran).

Cómo funcionan

Un portal cautivo se instala en la puerta de enlace de la red, que es el sitio por donde pasan los usuarios para acceder a Internet (puede ser un ordenador haciendo de router, o un router hardware).

El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente (haciendo lo que se llama Calidad de Servicio).

Usos

Se usan sobre todo en redes inalámbricas abiertas, donde interesa mostrar un mensaje de bienvenida a los usuarios y para informar de las condiciones del acceso (puertos permitidos, responsabilidad legal, etc.). Los administradores suelen hacerlo para que sean los propios usuarios quienes se responsabilicen de sus acciones, y así evitar problemas mayores. Se discute si esta delegación de responsabilidad es válida legalmente.

Dynamic Host Configuration Protocol

DHCP (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131. Para DHCPv6 se publica el RFC 3315.

Asignación de direcciones IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada computadora y, si la computadora se mueve a otra subred, se debe configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si fuera el caso en la computadora es conectada en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual o estática**: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
- **Asignación automática:** Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- **Asignación dinámica:** El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para

solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2136 (Inglés).

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (BootstrapProtocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

En Windows 98 o posterior, cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado "AutomaticPrivate Internet ProtocolAddressing".

Parámetros configurables

Un servidor DHCP puede proveer de una configuración opcional a la computadora cliente. Dichas opciones están definidas en RFC 2132 (Inglés)

- Lista de opciones configurables:
- Dirección del servidor DNS
- Nombre DNS

- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (broadcastaddress)
- Máscara de subred
- Tiempo máximo de espera del ARP (Protocolo de Resolución de Direcciones según siglas en inglés)
- MTU (Unidad de Transferencia Máxima según siglas en inglés) para la interfaz
- Servidores NIS (Servicio de Información de Red según siglas en inglés)
- Dominios NIS
- Servidores NTP (Protocolo de Tiempo de Red según siglas en inglés))
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor WINS

Implementaciones

Microsoft introdujo el DHCP en sus Servidores NT con la versión 3.5 de Windows NT a finales de 1994. A pesar de que la llamaron una nueva función no fue inventada por ellos.

El Consorcio de Software de Internet (ISC: Internet Software Consortium) publicó distribuciones de DHCP para Unix con la versión 1.0.0 del ISC DHCP Server el 6 de

diciembre de 1997 y una versión (2.0) que se adaptaba mejor al RFC el día 22 de junio de 1999. Se puede encontrar el software en http://www.isc.org/sw/dhcp/

Otras implementaciones importantes incluyen:

Cisco: un servidor DHCP habilitado en Cisco IOS 12.0 en el mes de febrero de 1999

Sun: añadió el soporte para DHCP a su sistema operativo Solaris el 8 de julio de 2001.

Además, varios routers incluyen soporte DHCP para redes de hasta 255 computadoras.

Accesos Públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

Administración

Este proceso lleva generalmente cuatro pasos:

- Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
- Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

ELEMENTOS QUE CONFORMAN UN CENTRO DE COMPUTO

INTERNET

Ilustración 3: Internet

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

ROUTER

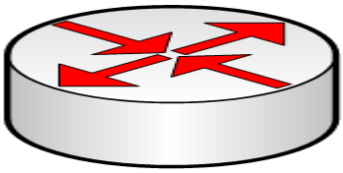

Ilustración 4: Router

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

El **enrutador** (calco del inglés*router*), **direccionador**, **ruteador** o **encaminador** es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

ETHERNET

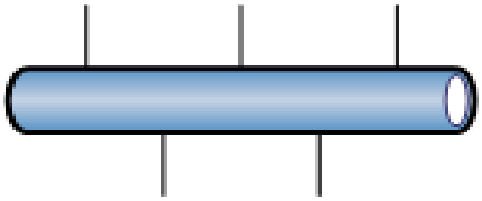

Ilustración 5: Ethernet

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. El nombre viene del concepto físico de *ether*. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

La Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos. Ambas se diferencian en uno de los campos de la trama de datos. Las tramas Ethernet e IEEE 802.3 pueden coexistir en la misma red.

SERVIDOR FIREWALL

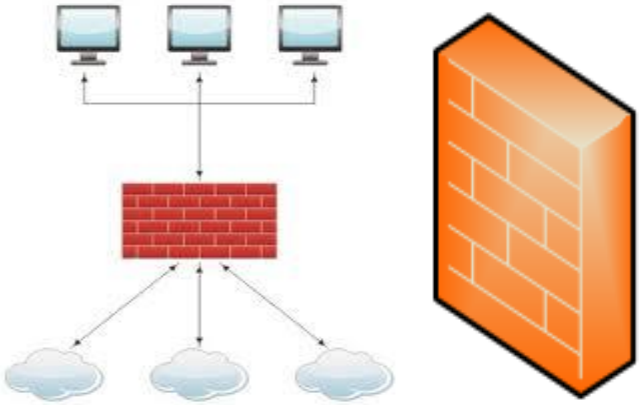

Ilustración 6: Firewall

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a este.

SERVIDOR DE ARCHIVO

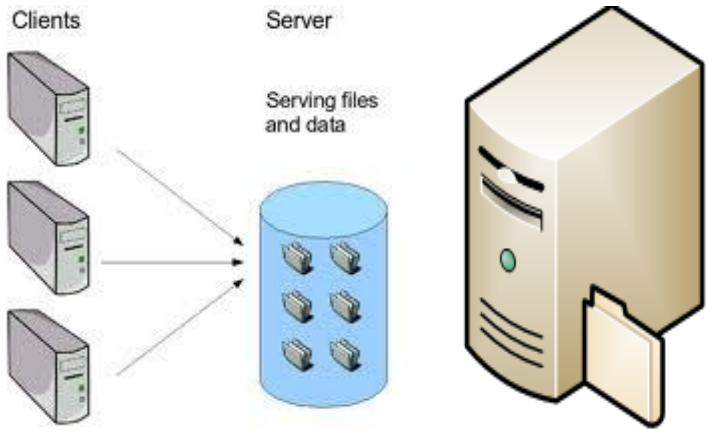

Ilustración 7: Servidor de Archivo

Elaboración: http://yabrembre.blogspot.com/2006/03/las-x-windows-i.html

Fuente: http://yabrembre.blogspot.com/2006/03/las-x-windows-i.html

Un servidor de archivos es una máquina de una red donde existen ficheros u otras máquinas, o clientes, pueden conectarse a ella y abrir, leer, escribir o manipular archivos. A menudo, por supuesto, el servidor de archivos y el cliente es la misma máquina, pero a veces no. Lo que el servidor de archivos está sirviendo es información en archivos.

SERVIDOR DE DOMINIO

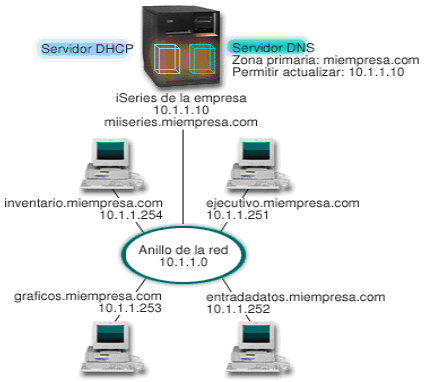

Ilustración 8: Servidor de Dominio

Elaboración:http://www.davidsuarez.es/2008/01/%C2%BFque-es-un-dns/

Fuente: http://www.davidsuarez.es/2008/01/%C2%BFque-es-un-dns/

Definición

Un servidor de DNS (Domain Name System) es capaz de recibir y resolver peticiones relacionadas con el sistema de nombres. Un servidor de DNS sirve, por tanto, para (1)

traducir su nombre de dominio en una dirección IP, (2) asignar nombres a todas las máquinas de una red y trabajar con nombres de dominio en lugar de IPs.

¿Cómo funciona?

Un servidor DNS permite acceder a un dominio en internet entre los millones existentes. Básicamente su función es atender a las peticiones hechas por los distintos programas que acceden a internet y resolver la dirección IP asociada al dominio consultado.

Cuando el servidor recibe una consulta realiza una búsqueda en caso de que ese servidor no disponga de la respuesta, el servidor comienza la búsqueda a través de uno o varios Servidores DNS hasta encontrar una respuesta positiva o negativa.

SERVIDOR DE APLICACIONES

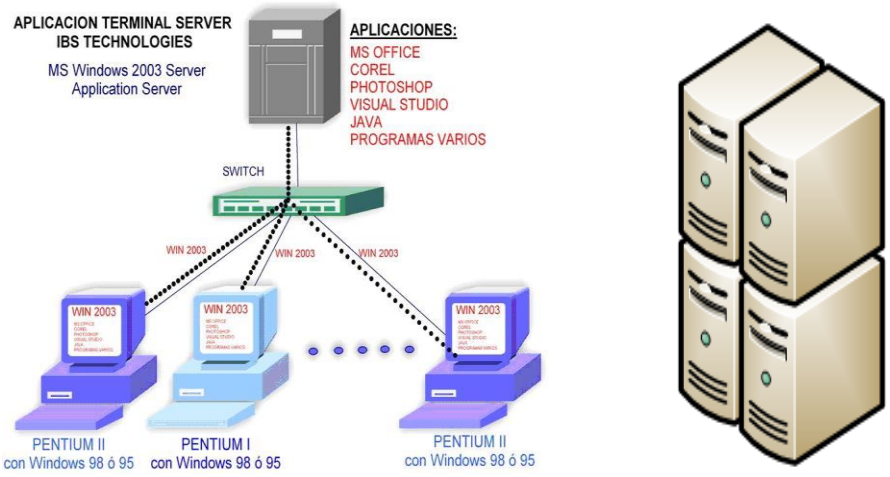

Ilustración 9: Servidor de Aplicaciones

Elaboración: http://www.quebarato.com.ar/

Fuente: http://www.quebarato.com.ar/

Tipo de servidor que permite el procesamiento de datos de una aplicación de cliente. Las principales ventajas de la tecnología de los servidores de aplicación es la centralización y la disminución de la complejidad del desarrollo de aplicaciones, dado que las aplicaciones no necesitan ser programadas; en su lugar, estas son ensambladas desde bloques provistos por el servidor de aplicación.

Ventajas de los servidores de aplicaciones

- Integridad de datos y códigos: al estar centralizada en una o un pequeño número de máquinas servidoras, las actualizaciones están garantizadas para todos sus usuarios. No hay riesgos de versiones viejas.
- Configuración centralizada: los cambios en la configuración de la aplicación, como mover el servidor de base de datos o la configuración del sistema, pueden ser hechos centralmente.
- Seguridad: se consideran más seguras.
- Performance: limitando el tráfico de la red solamente al tráfico de la capa de presentación, es percibido como un modelo cliente/servidor que mejora la performance de grandes aplicaciones.

SERVIDOR DE IMPRESIÓN

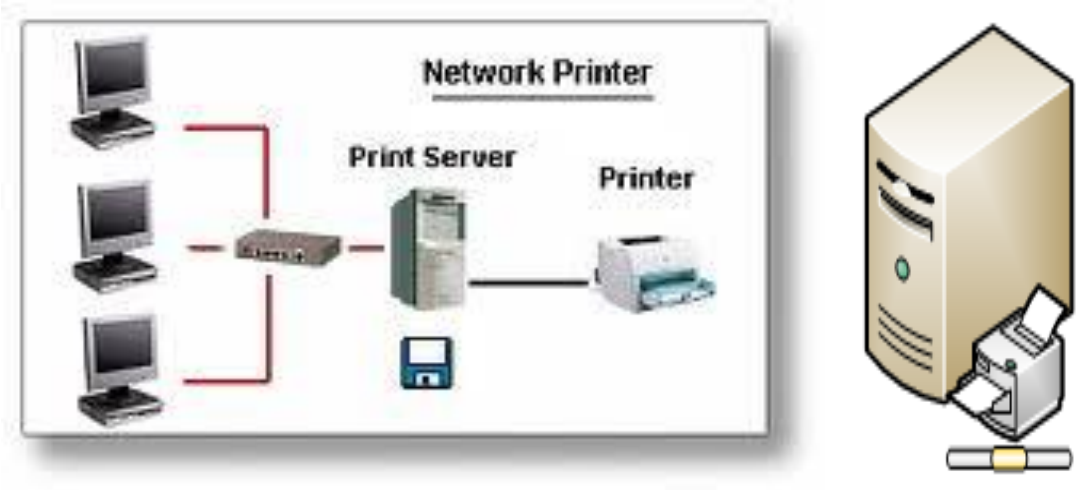

Ilustración 10: Servidor de Impresión

Elaboración: http://www.ecualug.org/

Fuente: http://www.ecualug.org/

Controla y maneja una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (Aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fue conectada directamente con el puerto de impresora del sitio de trabajo.

SERVIDOR DE CORREO

Ilustración 11: Servidor de Correo

Elaboración: http://www.linuxcentro.net

Fuente: http://www.linuxcentro.net

Almacenan, envían, reciben, enrutan, y realizan otras operaciones relacionadas con email para otros clientes en la red.

Servidor de fax: almacenan, envían, reciben, enrutan, y realizan otras funciones necesarias para la transmisión, la recepción, y la distribución apropiadas de los fax.

SERVIDOR DE BASE DE DATOS

Ilustración 12: Servidor de Base de Datos

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

SERVIDOR WEB

Ilustración 13: Servidor Web

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

SEVIDOR DE CONTENIDO

Ilustración 14: Servidor de Contenido

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

El servidor de contenido mantiene un depósito de contenidos, donde se almacenan tanto en su formato original como en formato de archivo visualizable en la Web.

SERVIDOR VOZ SOBRE IP

Ilustración 15: Servidor Voz sobre IP

Elaboración: Microsoft Visio

Fuente: Microsoft Visio

La **Voz sobre IP** o **Voz IP** consiste en transmitir voz sobre redes de datos usando una serie de protocolos para enviar la señal digital en paquetes en lugar de enviarla a través de circuitos analógicos conectados.

FUNDAMENTACIÓN LEGAL

Según el Reglamento de la Investigación Científica y Tecnológica de la Universidad de Guayaquil:

Título Preliminar

Disposiciones Fundamentales

Objetivo De La Investigación Científica Y Tecnológica

Art. 1.-Los objetivos de la investigación en la Universidad de Guayaquil están concebidos como parte de un proceso de enseñanza único, de carácter docente investigativo, orientado según norma el Estatuto Orgánico, para permitir el conocimiento de la realidad nacional y la creación de ciencia y tecnología, capaces de dar solución a los problemas del país. Las investigaciones dirigidas a la comunidad tienen por finalidad estimular las manifestaciones de la cultura popular, mejorar las condiciones intelectuales de los sectores que no han tenido acceso a la educación superior; la orientación del pueblo frente a los problemas que lo afectan; y la prestación de servicios, asesoría técnica y colaboración en los planes y proyectos destinados a mejorar las condiciones de vida de la comunidad.

Capítulo IV

Coordinación De Investigación De Las Unidades Académicas

Art. 14.-Las unidades académicas son responsables de la labor investigativa de sus Profesores (as) e Investigadores (as), y trabajarán por lograr la mayor integración posible de los proyectos de investigación a las necesidades del desarrollo científico y metodológico del pregrado y el posgrado, y a los fines de la formación integral y profesional de sus docentes y alumnos.

Según la Ley de Educación Superior:

Capítulo I

De la constitución, fines y objetivos del sistema nacional de educación superior

Art.3.- Las instituciones del Sistema Nacional de Educación Superior ecuatoriano, en sus diferentes niveles, tienen los siguientes objetivos y Estrategias fundamentales:

e) Desarrollar sus actividades de investigación científica en armonía con la legislación nacional de ciencia y tecnología y la Ley de Propiedad Intelectual.

Sección Novena

De la Ciencia y Tecnología

Art. 80.- El Estado fomentará la ciencia y la tecnología, especialmente en todos los niveles educativos, dirigidos a mejorar la productividad, la competitividad, el manejo sustentable de los recursos naturales y a satisfacer las necesidades básicas de la población.

La investigación científica y tecnológica se llevará a cabo en las universidades, escuelas politécnicas, institutos superiores técnicos y tecnológicos y centros de investigación científica, en coordinación con los sectores productivos cuando sea pertinente, y con el organismo público que establezca la ley, la que regulará también el estatuto del investigador científico.

Según la Ley de Propiedad Intelectual:

Sección V

Disposiciones Especiales sobre ciertas Obras

Art. 28. Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido

incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Según el Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

VARIABLES DE LA INVESTIGACIÓN

Las variables que se identifican en el presente proyecto son:

Variable Independiente: Análisis y Diseño de la Seguridad de software.

Variable Dependiente: Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking

Variable Independiente:

Análisis y Diseño de la Seguridad de software

En el análisis se identificaran las funciones que se realizan dentro del departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking, revisando las políticas normas y protocolos de seguridad informática para evaluar las vulnerabilidades que llegase a tener el mismo.

Se realizará el diseño que cubra las vulnerabilidades que tiene el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking a través de políticas, normas y protocolos que se deberán cumplir para mejorar la seguridad del software.

Variable Dependiente:

Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking.

El Departamento Técnico de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking será el encargado de llevar los controles de seguridad informática que es la principal aspecto de esta dependencia.

CAPÍTULO III

METODOLOGÍA

DISEÑO DE LA INVESTIGACIÓN

MODALIDAD DE LA INVESTIGACIÓN

El presente proyecto corresponde a la modalidad de proyecto factible ya que se ha elaborado un diseño de políticas de seguridad con el cual se plantearan posibles soluciones y se disminuirá el riesgo de las vulnerabilidades encontradas en el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y Networking.

La información con la que fue elaborada se encontró en documentos y estudios ya realizados, además se recogieron muchos controles de seguridad y normas en textos, internet y revistas los cuales han servido de guía para una mejor elaboración de este proyecto de tesis.

Es el que permite la elaboración de una propuesta de un modelo operativo viable, o una solución posible, cuyo propósito es satisfacer una necesidad o solucionar un problema. Los proyectos factibles se deben elaborar

respondiendo a una necesidad específica, ofreciendo soluciones de manera metodológica. (1)

Tipo de Investigación

El tipo de investigación al que pertenece este proyecto de tesis se encuentra en la categoría de proyecto factible, ya que se elaborará una propuesta que permitirá satisfacer las necesidades de seguridad informática en software presentes en la Carrera de Ingeniería en Sistemas Computacionales y NetWorking.

También está enmarcado en el tipo de investigación por el lugar de campo ya que la información con la fue elaborada el análisis se recolecto de manera directa realizando entrevistas al personal del Departamento Técnico Informático de la CISC.

POBLACION Y MUESTRA

POBLACIÓN

Definición: La población constituye el objeto de la investigación, siendo el centro de la misma y de ella se extrae la información requerida para el estudio respectivo, es decir el conjunto de individuos, objetos, entre otros, que siendo sometidos al estudio, poseen características comunes para proporcionar los datos, siendo susceptibles de los resultados alcanzados. (Mendoza, 2006)

Para este proyecto se ha tomado como población al personal con el que consta el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking, el cual está conformado por coordinadores, ayudantes y pasantes quienes son los encargados del manejo del centro de cómputo y los responsables de las actividades tales como implementación de políticas de seguridad, controles y demás procedimientos que se realizan dentro del Departamento Técnico Informático.

OPERACIONALIZACIÓN DE VARIABLES

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
V. I. Análisis y Diseño de la Seguridad Informática de software En el análisis se identificaran las funciones que se realizan dentro del departamento Técnico Informático de la CISC, revisando las políticas normas y protocolos de seguridad informática para evaluar las vulnerabilidades que llegase a tener el mismo. Se realizará el diseño que cubra las vulnerabilidades que tiene el Departamento Técnico Informático de CISC a través de políticas, normas y protocolos que se deberán cumplir para mejorar la seguridad del software.	Evaluación de la seguridad del área software.	Vulnerabilidades en varios controles de seguridad. Falta de planes de contingencia.	Entrevistas realizadas al personal del departamento técnico de la CISC.
	Diseño de la seguridad de software.	Falta de controles de seguridad informática en software.	Estudios realizados a otras instituciones. Consulta a expertos.

Elaboración: Investigador

Fuente: Investigador

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
V.D. Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking El Departamento Técnico de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking será el encargado de llevar los controles de seguridad informática que es el principal aspecto de esta dependencia.	Servicios ofrecidos por el departamento técnico informático de la CISC.	Tareas realizadas en el área de software.	Bibliografía especializada, consulta a expertos.
	Tecnología	Que posee el departamento para cubrir las necesidades y tener una mejor seguridad.	Entrevistas y estudios realizados a otras instituciones.

Elaboración: Investigador

Fuente: Investigador

TECNICAS DE RECOLECCIÓN DE DATOS

La recolección de datos es la parte fundamental de la investigación ya que por medio de estas técnicas podemos recopilar la información necesaria para la elaboración de nuestro análisis real.

Es muy importante ya que con la recolección de los datos en este proyecto analizaremos la situación actual de nuestro lugar de estudio, la técnica que se ha utilizado es la de campo ya que los hechos se captan tal y como se van presentando en el mismo sitio donde se encuentran el áreaestudiaday se puede observar cómo se desarrollan cada una de las actividades.

INSTRUMENTOS DE LA RECOLECCIÓN DE DATOS

Para el desarrollo de este proyecto se utilizaron técnicas para la recolección de datos que permitieron recolectar la información adecuada para un mejor entendimiento de las tareas que se desarrollan dentro del Departamento Técnico Informático de la CISC.

De esta forma podemos definir que "**Un instrumento de recolección de datos es en principio cualquier recurso de que pueda valerse el investigador para acercarse a los fenómenos y extraer de ellos información".... "De este modo el instrumento**

sintetiza en si toda la labor previa de la investigación, resume los aportes del marco teórico al seleccionar datos que corresponden a los indicadores y, por lo tanto a las variables o conceptos utilizados" (Carlos Savino: 149,150)

El instrumento que se ha utilizado para la recolección de datos del presente proyecto es la entrevista no estructurada ya que se intercambió información de forma verbal con los entrevistados se realizaron preguntas abiertas para que exista una mayor libertad y fluidez en la información que se está proporcionando.

Un punto muy importante es garantizar la confiabilidad y la validez de esta investigación que sirve para evaluar los instrumentos de recolección de datos que está empleando en investigador.

La validez de una investigación sirve para verificar si los resultados que se encuentran son reales y si abarca lo que realmente se desea en nuestra investigación para esto se ha solicitado la opinión de expertos en el área de seguridad los cuales nos han proporcionado los detalles sobre temas de seguridad informática en software y de este modo realizar una mejor recolección de los datos.

El termino confiabilidad se refiere a la capacidad del instrumento para arrojar datos o mediciones que corresponden a la realidad que se pretende conocer, o sea, la

exactitud de la medición, así como a la consistencia o estabilidad de la medición en diferentes momentos.

TÉCNICAS E INSTRUMENTOS

Cuestionarios

Para la elaboración del presente proyecto se utilizó el cuestionario para la recolección de los datos en los cuales se utilizaron preguntas abiertas para que exista mayor detalle en las respuestas y así obtener la mayor parte de información requerida, con la cual se procederá a la elaboración del análisis de la situación actual del Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking, y así se reconocerán cuáles serán las vulnerabilidades que afectan la seguridad del software.

Entonces podemos definir un cuestionario como **"Documento constituido por un conjunto de preguntas orientadas a obtener información específica de lo que se investiga"**

Entrevistas

Las entrevistas fueron realizadas directamente al personal interno del departamento técnico informático de la CISC, con las cuales se conoció más detalladamente las funciones que se realizan dentro del mismo.

Podemos definir a la entrevista como "**el método que se utilizan para recabar información en forma verbal, a través de preguntas que propone el analista. Quienes responden pueden ser gerentes o empleados, los cuales serán parte del personal interno de una organización**"

PROCESAMIENTO Y ANÁLISIS

ANÁLISIS DEL DEPARTAMENTO TÉCNICO INFORMÁTICO

Para el siguiente análisis se realizó el levantamiento de información recolectando los datos de la manera directa entrevistando al personal del Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking.

El departamento Técnico Informático consta de 2 áreas:

- Áreas de Hardware o Soporte Técnico
- Área de Software o programación

Las cuales no están debidamente separadas, el acceso al Departamento Técnico Informático es restringido y solo pueden acceder:

- 2 Coordinadores
- 1 Programador
- 13 Pasantes o Ayudantes

Estos tienen acceso a los servidores ya que todos se convierten en administradores y no existe algún tipo de privilegios entre un usuario y otro. No se tiene aplicado ningún software que registre el acceso de los usuarios a los servidores, el control se lo lleva a través de LOGS[1] propios de los Sistemas Operativos.

---

[1]Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, etc.)

La red de la Carrera de Ingeniería en Sistemas Computacionales cuenta con la topología de Red Estrella Extendida la cual tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos los cuales son el centro de otra estrella. Generalmente el nodo central está ocupado por un router, y los nodos secundarios por switch. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local.

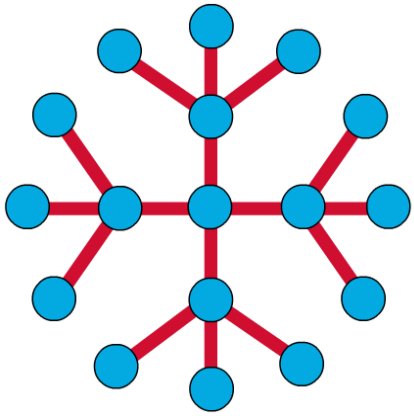

Ilustración 16: Ejemplo de topología de red en estrella extendida

Elaboración: http://tsminformatica.blogspot.com/

Fuente: http://tsminformatica.blogspot.com/

La red de la CISC cuenta con varias subredes tales como:

- Redes de Acceso
- Redes de Transporte
- Red de Administración o Intranet
- DMZ
- Core IP

RED DE ACCESO DE LA CISC

Las redes de acceso son las que tienen contacto con los usuarios finales, la Carrera de Ingeniería en sistemas computacionales consta de 5 laboratorios de los cuales 1 es inalámbrico

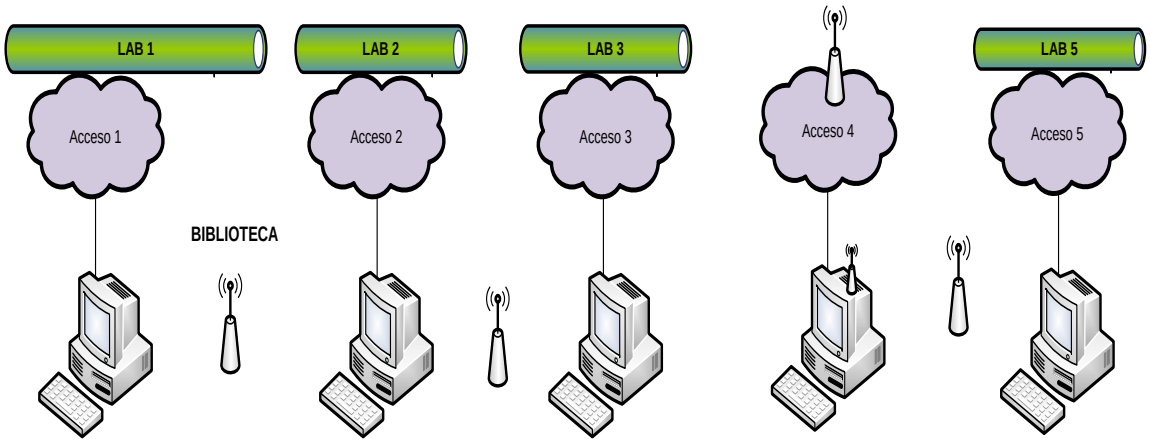

Ilustración 17: Red de acceso de la CISC

Elaboración: Investigador

Fuente: Investigador

Está comprendida por un 3Com Switch 3250 al cual le llega un enlace de cobre de la red de transporte, tiene 48 puertos 10/100 Mbps y dos 1000 o basados en SFP de fibra de puertos Gigabit full dúplex, la cobertura máxima de este servicio es de 100 metros.

RED DE TRANSPORTE DE LA CISC

Comprende una conexión principal de cobre que tiene como objetivo concentrar el tráfico de información que proviene de las redes de acceso, la cual comprende un nodo CISCO Catalyst 2950 de capa dos, tiene puntos de conexión de Fast Ethernet y Gigabit ethernet.

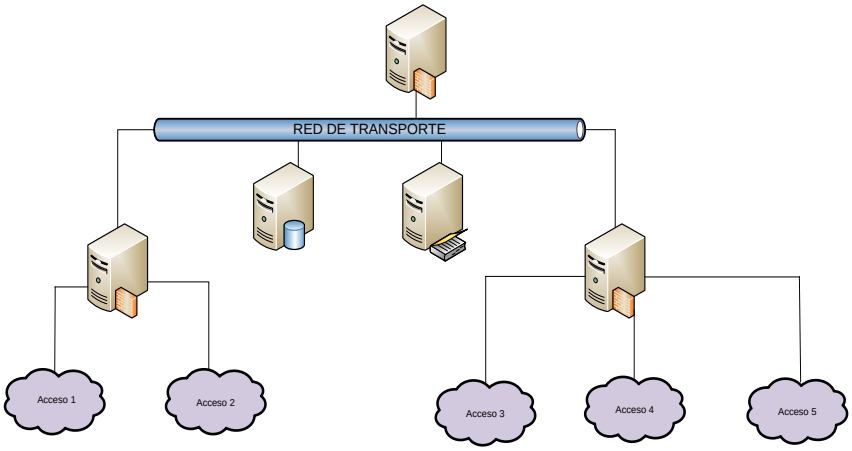

Ilustración 18: Red de transporte de la CISC

Elaboración: Investigador

Fuente: Investigador

SERVIDORES UTILIZADOS EN LA RED DE TRANSPORTE DE CISC

a. Dos servidores que funcionan como Routers a través del programa Quagga para los laboratorios por medio de los puertos zebra, ripd, squid - http, http proxyLógicos, dichos servidores usan el Sistema Operativo Centos 5.3.

#DE PUERTO	PUERTO
2601	Zebra
2601	Ripd
3128	Squid - Http
8080	Http proxy

b. Un servidor de base de datos destinada a la parte educativa de la carrera es decir para uso de los estudiantes cuenta con Sistema Operativo Centos 5.3, que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas.

RED DE ADMINISTRACION DE LA CISC

Esta red cuenta con el switch Cisco Catalyst 2950, con conexiones Fast Ethernet y Gigabit Ethernet para las estaciones de trabajo de la CISC, con una velocidad de transmisión configurada de 10/100/1000 Mbps full dúplex.

La red de Administración cuenta con los servidores de Web y Firewall, además están conectados 17 estaciones de trabajo y el Core IP a través de cable UTP.

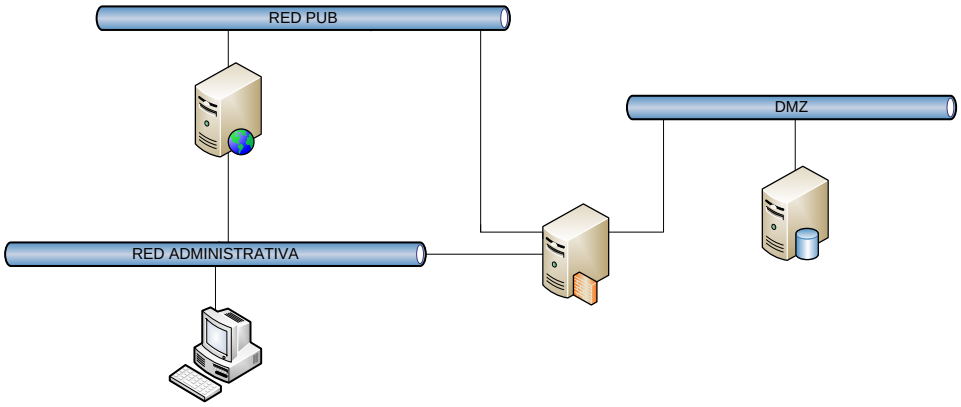

Ilustración 19: Red de Administración de la CISC

Elaboración: Investigador

Fuente: Investigador

SERVIDORES UTILIZADOS EN LA RED DE ADMINISTRACIÓN DE CISC

a. El Servidor web con Sistema Operativo Centos 5.3 se ejecuta en un ordenador manteniéndose a la espera de peticiones por parte de un cliente (un

navegador web) y que responde a estas peticiones adecuadamente, mediante una *página web* que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error.

# DE PUERTO	PUERTO
88/tcp	Open http
4444	Krbs
8009	Aip 13
8080	Http proxy

b. Servidor Firewall es un sistema diseñado para prevenir acceso no autorizado hacia o desde una red privada, usualmente sirve para proteger la red privada de una organización de las redes públicas o compartidas a las que se conecta, estos pueden ser implementados tanto en hardware como el software, o bien combinado los dos.

   La idea principal de un firewall es crear un punto de control de entrada y salida de tráficos de una red a través de políticas que se hayan definido de acuerdo a las necesidades de la organización. El servidor Firewall de la CISC cuenta con Sistema Operativo Centos 5.3

# DE PUERTO	PUERTO
2601	Zebra
2602	Ripd
3128	Squid – http
8080	Http proxy

c. A la red Administrativa de la CISC están conectadas además 17 estaciones de trabajo las cuales se detallan a continuación.

1. Coordinador de hardware
2. Coordinador de software
3. 3 estaciones de trabajo
4. Recepción
5. Dpto. de Subdirección
6. Coordinación
7. Biblioteca

ZONA DESMILITARIZADA

En seguridad informática, una **zona desmilitarizada** (DMZ, demilitarized zone) o **red perimetral** es una red local que se ubica entre la red interna de una organización

y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

En la red de la CISC se consta de u Switch Cisco Catalyst 2950 en el cual se ha implementado un VLAN la cual consta de la DMZ y la Zona PUB.

SERVIDORES CONECTADOS EN LA DMZ

a. Servidor de Base de Datos cuenta con Sistema Operativo Windows Server 2003 el cual es cual es utilizado en la red administrativa para datos de las transacciones internas de la CISC, este cuenta con las siguientes características.

CONEXIÓN A INTERNET

La conexión a Internet se establece con dos enlaces a través del proveedor TELCONET, con un ancho de banda de 3MB el cual se distribuye para todas las redes de la CISC.

a. La interface Fast Ethernet (publico) que es el primer enlace se la establece con el Router Cisco 851.
b. La interface Fast Ethernet (VPN) que es el segundo enlace se lo establece mediante un Router Cisco SB 101.

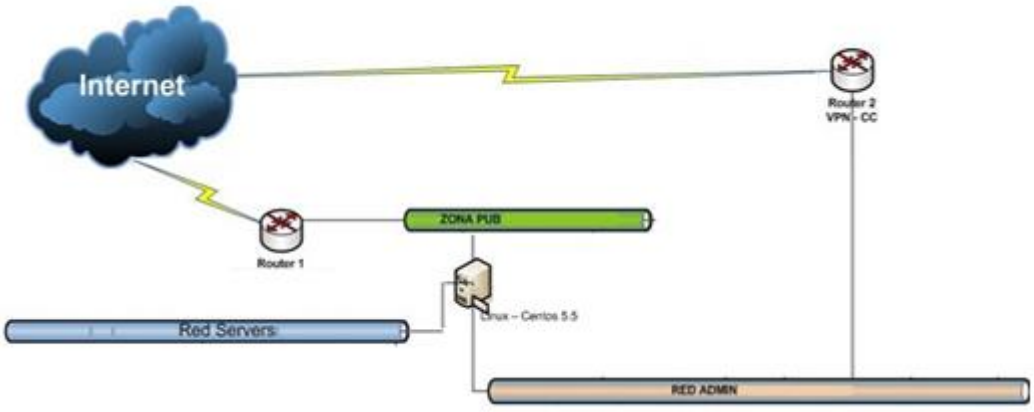

Ilustración 20: Conexión a Internet

Elaboración: Investigador

Fuente: Investigador

SOFTWARE EN SERVIDORES

Los Sistemas Operativos y Aplicativos son escogidos luego de realizar análisis, investigaciones y pruebas en máquinas virtuales antes de implementarlo ya que se tiene acceso a los canales de distribución de los productos utilizados.

Las actualizaciones en los servidores se realizan cada 6 meses en la cual se verifican Parches que constan de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo; Servicios que son programas que se ejecutan en segundo plano y que ofrecen soporte para otras aplicaciones; e Implementación de Seguridad.

El Antivirus que se utiliza en los servidores Linux es ClamAV open source (GPL) para Unix (y Linux) cuyo principal objetivo es la integración con servidores de correo (análisis de ficheros adjuntos), las actualizaciones se realizan automáticamente. También se suele instalar Avast, Avira, AVG en otros en el resto de las computadoras ya que no se lleva un estándar, es decir se cambia en cualquier momento, tomando en cuenta que los antivirus que se utilizan son de licencia libre es decir que o tienen ningún costo.

SERVIDORES EXISTENTES EN LA CISC

NOMBRE DEL SERVIDOR	SISTEMA OPERATIVO UTILIZADO	COMPONENTES UTILIZADOS Y FUNCIONES

Servidor Firewall Principal	CENTOS 5.5	• Squid
		• Dansguardian
		• Zebra
		• Smtp – correo
		• Ssh Acceso Remoto
		• Web –Apache
		• Firewall
		  ○ Salida puerto 3128
		  ○ No conexión externa

Servidores Firewall Lab 1,2	CENTOS 5.5	• Squid • Dansguardian • Zebra • Ssh Acceso Remoto • Web –Apache
Servidor Firewall Lab 3,4,5	CENTOS 5.5	• Squid • Dansguardian • Zebra • Ssh Acceso Remoto • Web –Apache
Servidor Oracle	RED HAT 5.0	• Base de Datos conexión solo para estudiantes que reciben cátedras.
Servidores de Base de Datos SQL Server 2005	WINDOWS SERVER 2003	• Conexión de base de datos de la CISC • Solo acceso interno • No acceso a otras subredes
Servidor Dominio	WINDOWS SERVER 2003	• Active Directory • DHCP (Usuarios Externos) • Firewall de Windows • Reparte ip solo administrativa (FIJA)

NOMBRE DEL SERVIDOR	SISTEMA OPERATIVO UTILIZADO	FUNCIONES
Servidor Trixbox		• Está configurado pero actualmente no se encuentra en producción.
Servidor de Evaluación Docente	WINDOWS SERVER 2003	• Se guarda la evaluación que realizan los estudiantes via web.
Laboratorios (Administradores)	UBUNTU 10.4	• Administradores laboratorios
Laboratorios (Clientes)	Windows XP	• Uso de estudiantes
Equipos personal administrativo	Windows 7	• Personal administrativo
Servidor Web	CENTOS 5.4	• Apache • Jboss • Firewall o Restricción de conexión externa Solo conexión de servidor de Base de Datos
Servidor de Información (Envío de Información a la Ciudadela Universitaria)	WINDOWS SERVER 2003	• Conectado a través de VPN o Sistema de la Universidad de Guayaquil.

COMPONENTES UTILIZADOS EN LOS SERVIDORES DE LA CISC

Squid

Programa de software libre que implementa un servidor proxy y un *dominio* para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a

DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

DansGuardian

Es un software de control de contenidos, diseñado para controlar el acceso a sitios web. Incluye un filtro de virus, importante en sistemas Windows, es usado principalmente en instituciones de educación, gobierno y empresas. Se caracteriza por su alto grado de flexibilidad y adaptación de la implementación.

Zebra (Administrador de Rutas)

Zebra es el corazón de Quagga y funciona como el administrador del ruteo IP. Este brinda las actualizaciones a las tablas de ruteo del kernel, lookups en la interface y la redistribución de rutas entre los diferentes protocolos.

Zebra instala cinco demonios que se escuchan en puertos consecutivos. A continuación una tabla muestra quales son los demonios y en que puertos escuchan:

Quagga

Es un paquete de software de encaminamiento que proporciona enrutamiento basado en servicios de TCP/IP con protocolos que soportan RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, quagga también soporta el comportamiento especial de BGP Router Reflector y Router Server. Además de enrutamientos basados en IPv4 y IPv6.
Quagga es un fork de GNU Zebra con la intención de ser utilizado como un servidor de rutas y reflector.

RIPD

Protocolo de información de enrutamiento, es un protocolo de pasarela interior ampliamente desplegado, un router funcionando con RIP envía actualizaciones a sus vecinos periódicamente, permitiendo la convergencia así a una topología conocida. En cada actualización la distancia de una red dada será comunicada a todos los demás routers vecinos del mismo.

SSH

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host

remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

SMPT

(Simple Mail Transfer Protocol).Protocolo Simple de Trasferencia de Correo. Protocolo que se usa para trasmitir correo electrónico entre servidores.

POP 3

(Post Office Protocol 3 - Protocolo 3 de Correo). Es un protocolo estándar pararecibir mensajes de e-mail. Los mensajes de e-mails enviados a un servidor, son

almacenados por el servidor pop3. Cuando el usuario se conecta al mismo (sabiendo la dirección POP3, el nombre de usuario y la contraseña), puede descargar los ficheros.

ACTIVE DIRECTORY

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory está basado en una serie de estándares llamados (X.500), aquí se encuentra una definición lógica a modo jerárquico.

Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

A su vez, los árboles pueden integrarse en un espacio común denominado bosque (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de «trust» o confianza entre ellos. De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio Active Directory.

DHCP

DHCP (**Dynamic Host ConfigurationProtocol**) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet. Una dirección IP es análoga a un número de teléfono.

La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

SEGURIDAD EN SERVIDORES

Entre los proyectos de seguridad que se han implemento esta:

Hardening en Linux que es una técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo

posible la seguridad de este. Entre sus controles de seguridad implementados en el sistema destacan:

- Prevención de la ejecución del código arbitrario.
- Control de ejecución de las tareas en el stack.
- Restricción que permite que un usuario visión solamente su procesos.
- Control de las actividades de los usuarios.
- Permisos de ejecución en determinadas áreas del sistema.
- La protección a nivel de funcionamiento del kernel.
- Implementación de controles adicionales a la seguridad impuesta por chroot.
- Alarmas e intervenciones de seguridad que contienen el IP del que causa la alarma.
- Implementación de un control de acceso basado en roles (RBAC).

Hardening en Windows es reducir las posibilidades de éxito de un ataque, eliminando software, usuarios, servicios innecesarios y aplicando diariamente el sentido común en las tareas que realizamos. Este punto consiste en diferentes pasos que pasaremos a detallar.

- Use una cuenta con pocos privilegios (no administrador)
- Active el firewall
- Habilitar Updates Automáticos y actualizar a Microsoft Updateengine

- Desinstalar Software y Servicios que no utilice
- Verificar updates de software de terceros
- Habilitar Full Data Execution Prevention
- Instalar un Antivirus
- Deshabilitar o Restringir el Autoplay
- Utilizar herramientos de Webfiltering

También se cuenta con la implementación de *Reglas de Firewall*, contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (*permitir*)
- Bloquear la conexión (*denegar*)
- Rechazar el pedido de conexión sin informar al que lo envió (*negar*)

Políticas de Acceso y SELinux que es una colección de parches que modifican el núcleo del sistema operativo Linux, fortaleciendo los mecanismos de control de acceso y forzando la ejecución de los procesos dentro de un entorno con los mínimos privilegios necesarios. No se ha aplicado ningún sistema detector de intrusos.

Entre otros controles de seguridad del Departamento Técnico Informático podemos mencionar las siguientes políticas básicas las cuales se encuentran debidamente documentadas y aplicadas tales como:

- Autenticación
- Contraseñas a Nivel de Bios
- Contraseñas a Nivel Operacional
- Lista de control de Acceso y Navegación
- Filtros de Conexión a Nivel de Protocolos dinámicos
- VLAN
- Subnetting en las todas las redes

Se cuenta con reglamento para usuarios, administrador y políticas estipuladas dentro del departamento los cuales son respetados por todos.

RESPALDO DE INFORMACIÓN

A pesar de la importancia que tiene la información en un centro de cómputo en el Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales y NetWorking no se le da la importancia requerida tal es el caso que el respaldo de información se realiza anualmente y el mismo no se encuentra guardado en un lugar adecuado ni cuentan con las medidas de seguridad necesarias, tampoco se lleva un control estricto de las copias de estos archivos es decir, no se realizan auditorias periódicas a los medios de almacenamientos. Cabe recalcar que el almacén de los archivos de respaldo se encuentra en el mismo lugar donde se encuentra el Departamento Técnico Informático.

Otro punto muy importante es que en caso de préstamo de información no existe un procedimiento o un registro que identifique ¿Qué? o ¿A quién?, se prestó dicha información es decir no se lleva un control de préstamos de archivos en el departamento técnico, esto puede ser la causa de pérdida o fuga de información relevante. Se utiliza la política de conservación de archivos Hijo-Padre-Abuelo, y no se destruye nunca un respaldo.

SOFTWARE ACADÉMICO

En la Carrera de Ingeniería en Sistemas Computacionales y NetWorking se han desarrollado varios aplicativos para uso interno en la institución los cuales se detallan a continuación.

APLICATIVO	DESCRIPCION	LENGUAJE DE PROGRAMACIÓN	BASE DE DATOS
Integrador	Software principal es usado en la parte académica (semestre, preuniversitario, graduación, Academia Visual Basic 6.0Cisco, Recaudación).	Visual Basic 6.0	SQL Server 2000
Sistema de Compras	Para compras menores de $200.00 y pago de proveedores	Visual Basic 6.0	SQL Server 2000
EvaCisc	Evaluación Docente via web	JSP (Java)	SQL Server 2000
Cisc Académico	Sistema Académico via web	JSP (Java)	SQL Server 2000
Académico del CC	Centro de computo de la Administración central: Información de, Docentes, estudiantes(calificaciones, órdenes de pago)	Visual Basic 6.0	SQL Server 2000
Recaudaciones del CC	Centro de computo de la Administración central: Traspasos de cobros.	Visual Basic 6.0	SQL Server 2000
Adquisiciones	Solicitudes de compras superiores a $ 2000.00 Cobros.	Visual Basic 6.0	SQL Server 2000

APLICATIVO	DESCRIPCION	LENGUAJE DE PROGRAMACIÓN	BASE DE DATOS
Recursos Humanos	Incluye asistencia y contratos.	Visual Basic 6.0	SQL Server 2000
Test (Test de Actitud)	Aplicar test de actitud a los estudiantes antes de ingresar al Pre-Universitario		

Los proyectos de desarrollo son autorizados por las autoridades de la CISC, el recurso humano se asigna de acuerdo a la afinidad con el proyecto para que sea más productivo, el tiempo de duración se estima de acuerdo al proyecto, el presupuesto se lo calcula en base a los recursos, y el control de los avances del proyecto de lo realiza de acuerdo al cronograma.

Al momento de implementar la aplicación se realizan capacitación a los usuarios además se entrega un manual de usuario y una memoria técnica.

SOFTWARE DE APLICACIONES

Las aplicaciones instaladas en las computadoras de la CISC son de acuerdo a las necesidades de los estudiantes y siempre están actualizadas es decir que se instala última versión, las aplicaciones no tienen licencia ya que se utilizan aplicaciones gratis o se instalan con un crack que les permite la utilización de la aplicación.

FUNCIONES DEL COORDINADOR DE SOFTWARE

1. Elaborar el Plan Estratégico del Área de Software de la Carrera de Ingeniería Computacionales.
2. Asesorar al subdirector en el área académica en las asignaturas que tienen relación con temática de Software.
3. Colaborar con la planificación y desarrollo de eventos Científicos – Técnicos de informática.
4. Proveer asistencia y asesoría técnica, atendiendo los requerimientos de las autoridades de la Carrera.
5. Redactar informes de factibilidad técnica para conocimiento y toma de decisiones de la Dirección y/o Subdirección.
6. Informar a la Dirección de la carrera sobre las necesidades de Recursos Humanos y/o materiales inherentes a sus funciones.
7. Presidir la Comisión Técnica y concurrir a las sesiones de Comisión Académica cuando fuere invitado.
8. Informar oportunamente a la Dirección o Subdirección, acerca de las incidencias y conclusiones de cada reunión técnica.
9. En conjunto con el Coordinador de Hardware, liderar la instalación y puesta a punto, de los sistemas informáticos necesarios para el ejercicio de la Cátedra.
10. Controlar la correcta administración del Software instalado.

11. Contribuir y participar con el proceso de matriculación, cuando las autoridades lo requieran.
12. Interactuar periódicamente con los usuarios en la definición de sus necesidades y en los procesos de automatización, acordes a los estándares establecidos.
13. Estudiar, analizar y diseñar las propuestas de solución a los problemas o requerimientos de los sistemas informáticos existentes o la creación de nuevos módulos y/o aplicaciones.
14. Informar a la dirección sobre la mejor solución informática, especificando la situación actual del problema, causas y consecuencias del requerimiento, tiempo de desarrollo, fases de prueba, fecha máxima de puesta en producción.
15. Coordinar la implantación de las soluciones y requerimientos a los sistemas informáticos existentes en la carrera, consultando con el coordinador de hardware.
16. En conjunto con el Coordinador General de Graduación, realizar actividades del Curso de Graduación o Tesis de Grado con la finalidad de conocer los alcances y la documentación técnica de los Proyectos de Graduación; de tal forma que pueda coordinar, de ser factible con los respectivos autores e institución beneficiaria, el proceso de implantación de los sistemas informáticos sustentados.
17. Planificar la capacitación y soporte técnico de los sistemas informáticos a los usuarios administrativos de la Carrera.

18. Realizar pruebas de control de calidad de las aplicaciones informáticas generadas en conjunto con la Coordinación de los Laboratorios.
19. Supervisar a los Programadores la elaboración de la Documentación Técnica, de procedimientos y de usuarios de los Sistemas Computacionales.
20. Administrar y monitorear la Base y Red de datos de la Carrera de Ingeniería en Sistemas Computacionales.
21. Elaborar el Plan de seguridad, Contingencias y Desastres para preservar la continuidad de las operaciones automatizadas de la Carrera.
22. Controlar la correcta administración y actualización del Sitio Web de la carrera de Ingeniería en Sistemas Computacionales.
23. Participar en el proceso de evaluación de clase demostrativa del profesional aspirante a Docente del área de informática.
24. Análisis, diseño e implantación de soluciones informáticas a nivel administrativo.
25. Presentar en la Dirección de la Carrera, el informe anual (de Enero a Diciembre), referente a las actividades cumplidas.
26. Cualquier otra actividad que la autoridad lo solicite.

DESCRIPCIÓN DE LAS POLITICAS DE SEGURIDAD QUE DEBE TENER EL CENTRO DE CÓMPUTO

¿Qué son las Políticas de Seguridad?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

Seguridad Lógica

Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

¿Qué son las Normas de Seguridad?

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

Responsabilidades

El Responsable de Seguridad Informática estará a cargo de:

- ✓ Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; la solicitud y aprobación de accesos a Internet; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- ✓ Definir pautas de utilización de Internet para todos los usuarios.
- ✓ Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- ✓ Controlar la asignación de privilegios a usuarios.
- ✓ Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- ✓ Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- ✓ Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- ✓ Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- ✓ Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- ✓ Evaluar los riesgos a los cuales se expone la información con el objeto de:
    - o Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.

- Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

- ✓ Aprobar y solicitar la asignación de privilegios a usuarios.
- ✓ Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- ✓ Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las Unidades Organizativas, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área Informática cumplirá las siguientes funciones:

- ✓ Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- ✓ Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- ✓ Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- ✓ Implementar el control de puertos, de conexión a la red y de ruteo de red.
- ✓ Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- ✓ Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- ✓ Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- ✓ Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

- ✓ Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- ✓ Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- ✓ Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

DISEÑO DE LAS POLITICAS DE SEGURIDAD

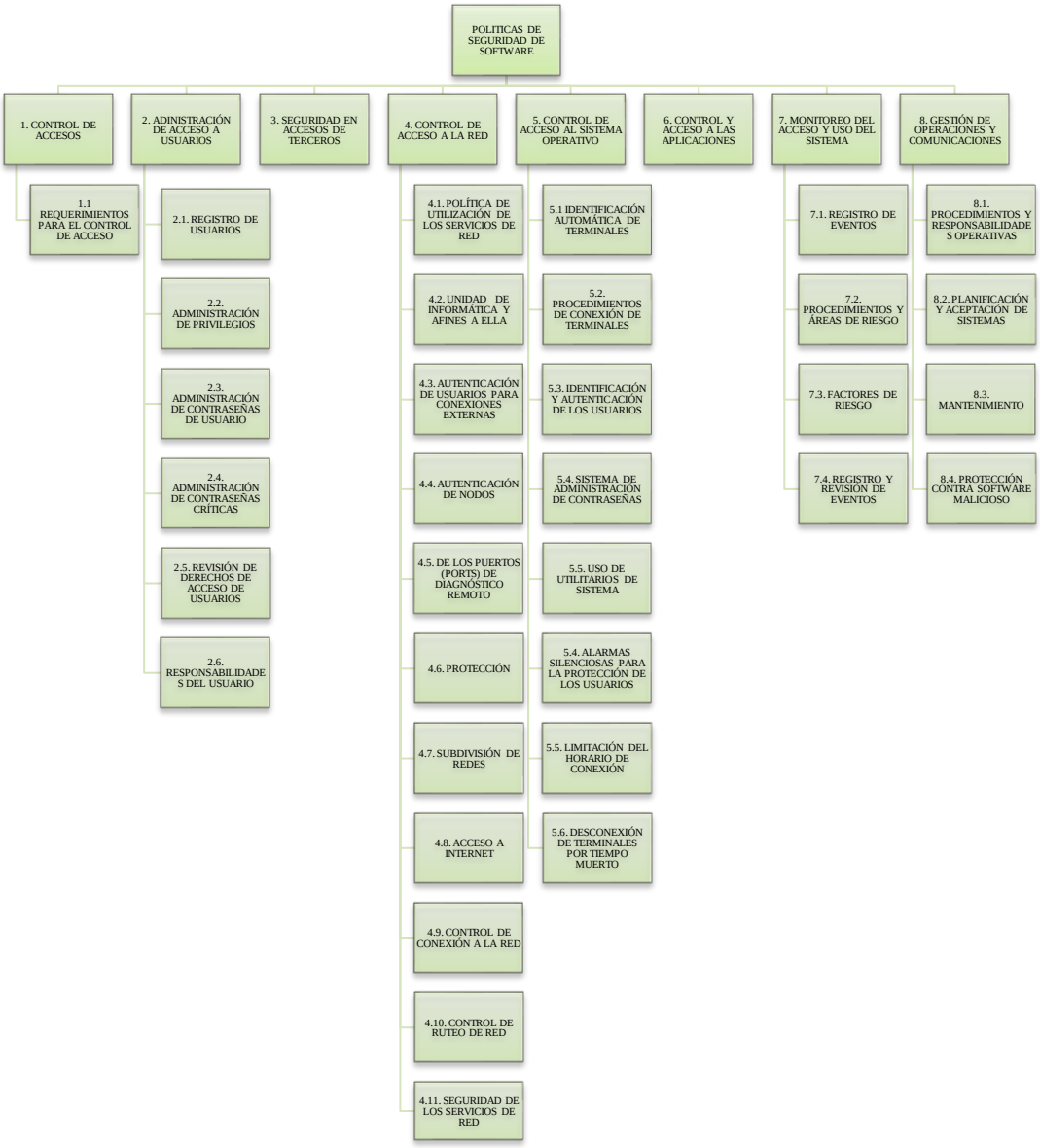

Ilustración 21: Políticas generales de seguridad informatica

Elaboración: Investigadora

Fuente: Investigadora

NIVEL DE SEGURIDAD LÓGICO

1. Control de Accesos

2. Administración del Acceso de Usuarios

3. Seguridad en Acceso de Terceros

4. Control de Acceso a la Red

5. Control de Acceso a los Sistemas Operativos

6. Control de Acceso a las Aplicaciones

7. Monitoreo del Acceso y Uso del Sistema

8. Gestión de operaciones y comunicaciones

9. Desarrollo y Mantenimiento de los Sistemas

1. CONTROL DE ACCESOS

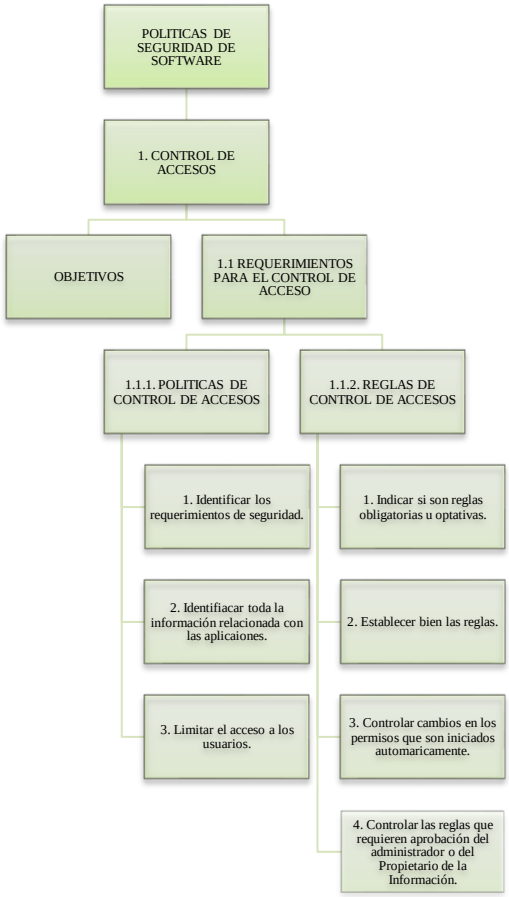

Ilustración 22: Diseño de políticas de control de acceso

Elaboración: Investigadora

Fuente: Investigadora

Objetivo

- ✓ Restringir el acceso a los sistemas de información, bases de datos y servicios de información.

- ✓ Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- ✓ Vigilar la seguridad de conexión entre la Institución y otras redes públicas o privadas.
- ✓ Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

1.1. Requerimientos para el Control de Acceso

1.1.1. Política de Control de Accesos

Se debe contemplar los siguientes aspectos:

1. Identificar los requerimientos de seguridad de las aplicaciones.
2. Identificar toda la información relacionada con las aplicaciones.
3. Limitar el acceso de los usuarios de acuerdo a los perfiles de usuarios de acuerdo a la categoría de puestos de trabajo.

1.1.2. Reglas de Control de Acceso

Las reglas deberán:

1. Se debe indicar si las reglas son obligatorias u optativas.

2. Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.

3. Registrar los cambios en los permisos de usuario que se inician automáticamente con el sistema de información y aquellos que son iniciados por el administrador.

4. Definir que reglas requieren aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

2. ADMINISTRACIÓN DEL ACCESO DE USUARIOS

El principal objetivo es restringir el acceso a la información al personal no autorizado, por tal motivo se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

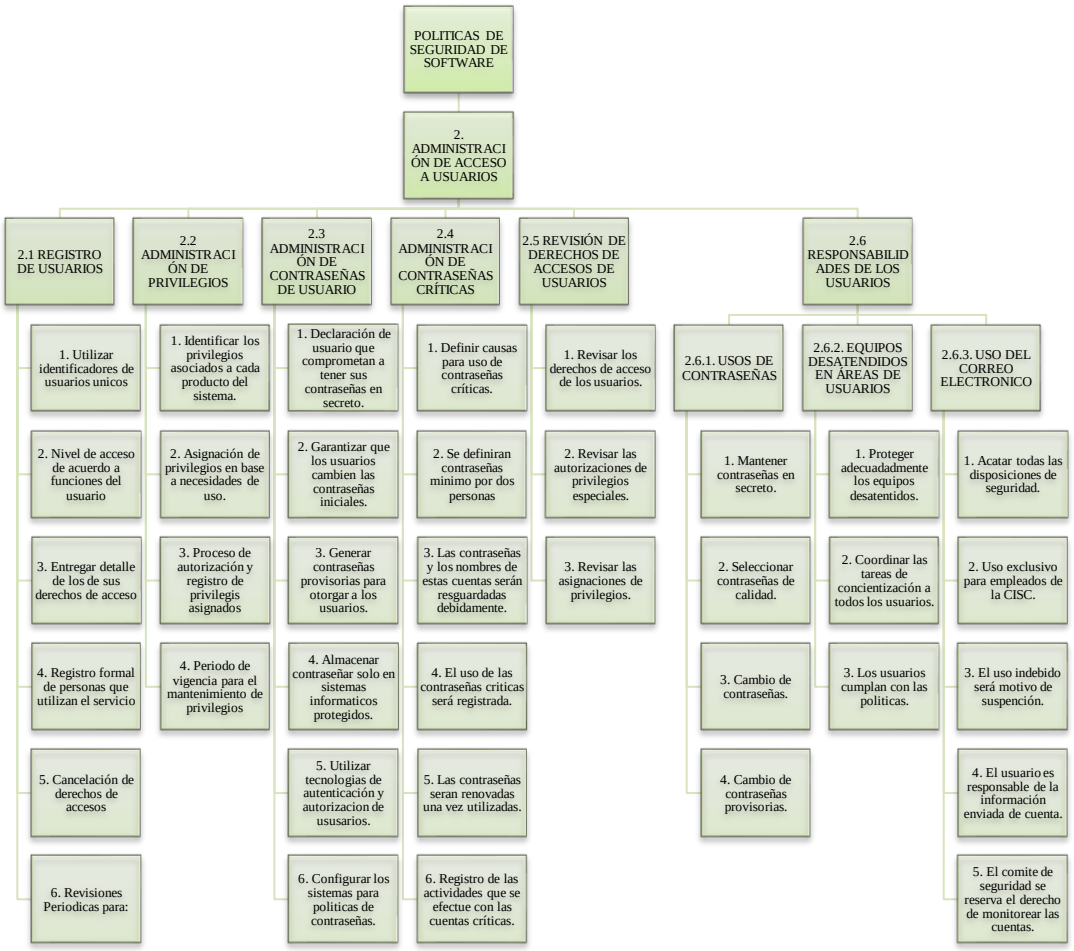

Ilustración 23: Diseño de políticas de administración del acceso de usuarios

Elaboración: Investigadora
Fuente: Investigadora

2.1. Registro de Usuarios

Se definirá un procedimiento formal de registro de usuario para permitir o no el acceso a todos los sistemas, base de datos y servicios de información el cual será realizado por el Responsable de Seguridad Informática.

1. Asignar identificadores únicos para los usuario, para de esta forma poder identificar a los usuarios por sus acciones, también evitar la existencia de múltiples perfiles de acceso para un mismo usuario. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
2. Verificar que el nivel de acceso que se da a los usuarios es el apropiado para que este desempeñe adecuadamente sus funciones.
3. Entregar a los usuarios un detalle escrito de sus derechos de acceso.
4. Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
5. Inhabilitar inmediatamente los permisos de acceso de los usuarios que cambiaron sus funciones, o de aquellos a los que se les revocó la autorización, o se desvincularon de la Institución.
6. Realizar revisiones constantes con el objeto de:
    a. Eliminar identificadores y cuentas de usuario repetidas.
    b. Inhabilitar cuentas inactivas por más de 30 días.

c. Eliminar cuentas inactivas por más de 60 días.

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

1. Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
2. Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
3. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

4. Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

2.3. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

1. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
2. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
3. Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico

sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

4. Almacenar las contraseñas sólo en sistemas informáticos protegidos.
5. Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).
6. Configurar los sistemas de tal manera que:
    a. Las contraseñas tengan 8 caracteres mínimo
    b. Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),
    c. solicitar el cambio de la contraseña cada 30 días
    d. impedir que las últimas 6 contraseñas sean reutilizadas

2.4. Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o

sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

1. Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
2. Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
3. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
4. La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
5. Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
6. Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

2.5. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de 4 meses, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

1. Revisar los derechos de acceso de los usuarios a intervalos de 4 meses.
2. Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses.
3. Revisar las asignaciones de privilegios a intervalos de 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

2.6 Responsabilidades del Usuario

2.6.1. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

1. Mantener las contraseñas en secreto.

2. Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    a. Sean fáciles de recordar.
    b. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    c. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
3. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
4. Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

2.6.2. Equipos Desatendidos en Áreas de Usuarios

1. Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

2. El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.
3. Los usuarios cumplirán con las siguientes pautas:
    a. Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
    b. Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

2.6.3 Uso del correo electrónico

1. El servicio de correo electrónico, es un servicio gratuito, y no garantizable, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.
2. El correo electrónico es de uso exclusivo, para los empleados de la CISC y accionistas de la misma.

3. Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.
4. El usuario será responsable de la información que sea enviada con su cuenta.
5. El comité de seguridad, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

3. SEGURIDAD EN ACCESO DE TERCEROS

Ilustración 24: Diseño de políticas de seguridad en acceso a terceros

Elaboración: Investigadora

Fuente: Investigadora

1. El acceso de terceros será otorgado siempre que cumplan con los requisitos de seguridad que se deberán establecer en el contrato de trabajo, el cual deberá estar firmado por las entidades correspondientes.
2. El usuario externo, utilizará y será responsable única y exclusivamente el servicio que le fue asignado

4. CONTROL DE ACCESO A LA RED

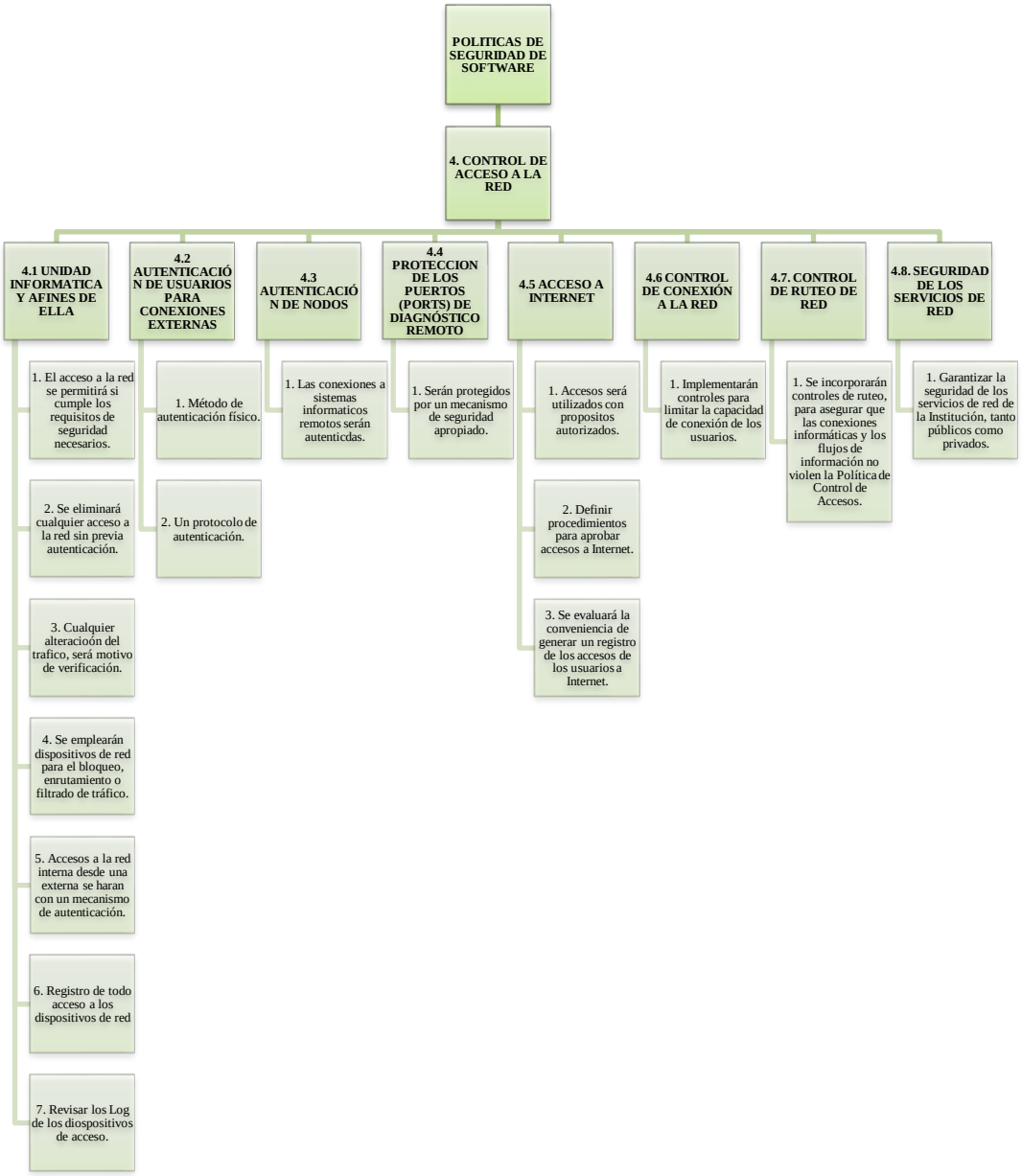

Ilustración 25: Diseños de políticas de control de acceso a la red

Elaboración: Investigadora

Fuente: Investigadora

4.1 Unidad de Informática y afines a ella.

1. El acceso a la red interna será permitido solo si se cumplen con los parámetros de seguridad establecidos los cuales serán permitidos por medio de un mecanismo de autenticación.
2. No se permitirá ningún acceso sin previa autenticación o validación del usuario o equipo.
3. Si se altera el tráfico entrante o saliente en la red se realizará una auditoría con la cual se determine el motivo y la actividad por la que se vio alterada la red.
4. Se tendrá que emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico para evitar el acceso o filtro de información que no este autorizada en la red interna o viceversa.
5. Accesos a la red interna desde una extranet, se realizaran mediante el mecanismo de autenticación seguro además el trafico entre ambas redes deberá ser cifrado con una encriptación de 128 bits.
6. Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o Log.
7. Se efectuará una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

4.2. Autenticación de Usuarios para Conexiones Externas

Los accesos a los usuarios remotos deberán cumplir procedimiento de autenticación. El responsable de la seguridad informática realizará una evaluación de riesgo a fin de determinar el mecanismo de identificación que corresponda a cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

1. Un método de autenticación físico, en los cuales se implementarán procedimientos tales como:
    a. Fijar la herramienta de autenticación.
    b. Registro de los que poseen autenticadores.
    c. Procedimiento de cancelación de acceso del autenticador.

2. Un protocolo de autenticación, en el cual se implementaran procedimientos que deberán establecer:
    a. Reglas con el usuario.
    b. Un ciclo de vida de las reglas para su renovación.

Los controles de re-llamada, o dial-back, ofrecen protección contra conexiones no deseadas a las instalaciones de procesamiento de información de la Institución. Al emplear este tipo de control, la Institución no debe utilizar servicios de red que contengan desvío de llamadas. Si por alguna debemos mantener el desvío de

llamadas, no será posible aplicar el control de re-llamada. Del mismo modo, es primordial que el proceso de rellamada garantice que se produzca una desconexión real del lado de la Institución.

4.3. Autenticación de Nodos

1. Con herramientas de conexión automática a una computadora remota se tendría un medio para obtener acceso no autorizado a una aplicación de la Institución. Por lo tanto todas las conexiones remotas serán autenticadas. Esto es importante si debemos usar una red que no se encuentra dentro de los controles de seguridad de la institución.

4.4. Protección de los Puertos (Ports) de Diagnóstico Remoto

En una red las computadoras y sistemas de comunicación se encuentran instalados y dirigidos con una herramienta de diagnóstico remoto. En el caso de no estar protegidos los puertos de este diagnóstico son vulnerables a accesos no autorizados. Por los tanto estos puertos serán protegidos con herramientas de seguridad apropiadas, con controles similares a los de “Autenticación de Usuarios para Conexiones Externas”.

4.5. Acceso a Internet

1. Se hará uso de este beneficio solo para los propósitos que fueron autorizados y destinados.
2. El encargado de definir los procedimientos para solicitar y aprobar el acceso a Internet será el Responsable de Seguridad Informática. Del mismo modo este especificará los patrones del uso de Internet para todos los usuarios.
3. Se generará un registro de los usuarios que tienen acceso a Internet para poder realizar controles de los accesos realizados y si es necesario revisar casos particulares, el responsable de Seguridad Informática implementará como firewall y proxies para efectivizar los controles.

4.6. Control de Conexión a la Red

1. Se implementarán controles para limitar la conexión de los usuarios. Estos controles deberán ser implementados en los "gateways" que separen cada uno de los dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a. Correo electrónico.
b. Transferencia de archivos.

c. Acceso interactivo.

d. Acceso a la red fuera del horario laboral.

4.7. Control de Ruteo de Red

1. A las redes que están fuera de la institución y las redes compartidas se le deberá incorporar políticas de ruteo de este modo se evitará que las conexiones y los flujos de información no infrinjan las políticas de control de acceso, las cuales examinaran minuciosamente las direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

4.8. Seguridad de los Servicios de Red

1. Se deberá establecer controles para garantizar los servicios de la red de la Institución tanto públicos como privados, el Responsable de Seguridad Informática junto con el Responsable del Área Informática serán los encargados de establecer dichos controles.

Los controles se deberán establecer tomando en cuenta las siguientes directivas:

a. Solo instalar y habilitar los servicios que necesariamente sean utilizados.

b. El uso y la administración de los servicios deberán ser controlados.

c. Para evitar las vulnerabilidades los servicios deben ser configurados de manera segura.

d. Instalar periódicamente las actualizaciones de seguridad.

Estas configuraciones serán revisadas periódicamente por el Responsable de Seguridad Informática.

5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

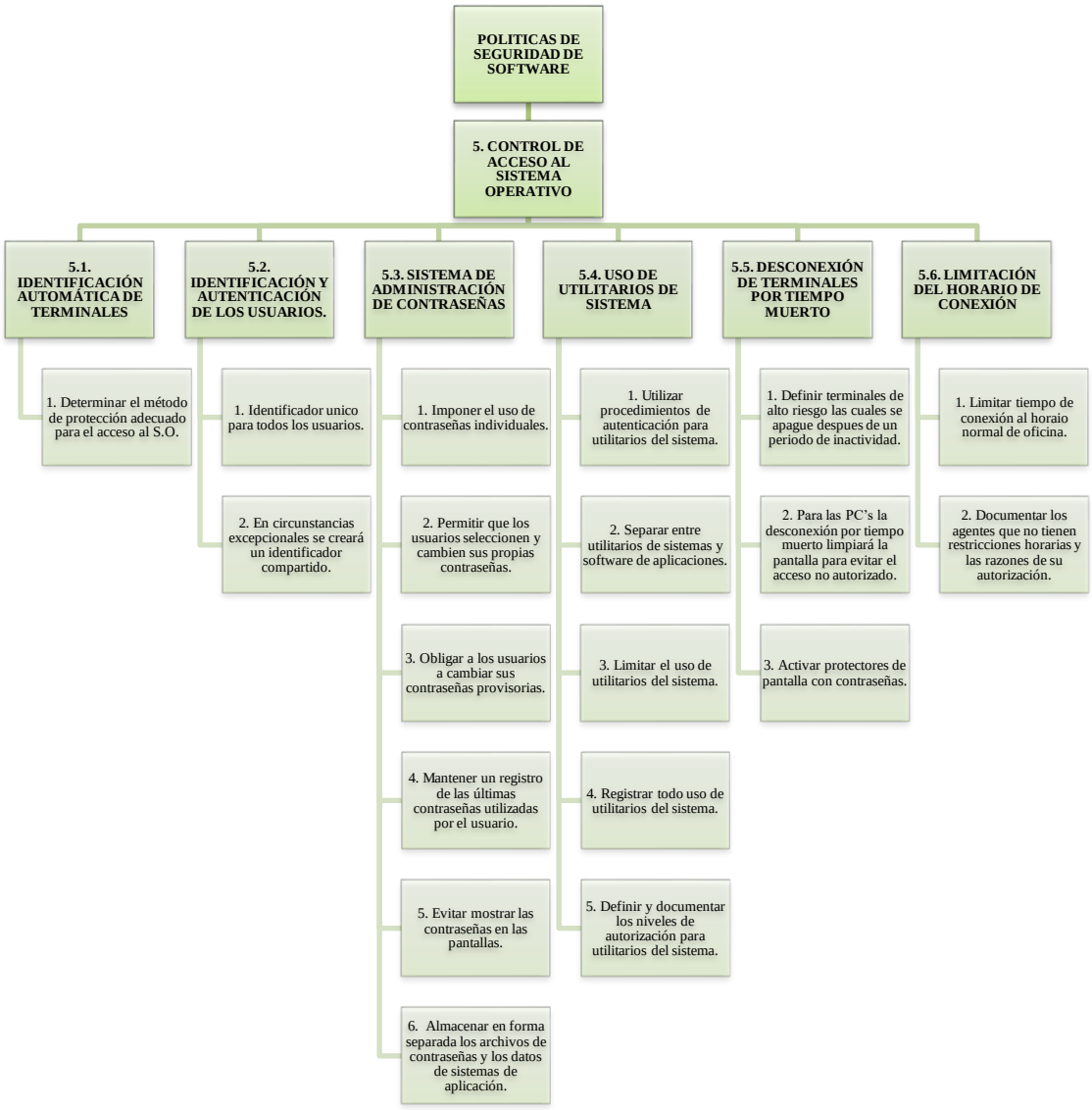

Ilustración 26: Diseño de políticas de control de acceso al sistema operativo

Elaboración: Investigadora

Fuente: Investigadora

5.1. Identificación Automática de Terminales

1. Realizar una evaluación de riesgos con el cual se determinará el método apropiado de protección para el acceso al sistema operativo.

   Si dicha evaluación diera como resultado que existe la necesidad de implementar un método de identificación de terminales, los procedimientos indicaran:

   a. El método de identificación automática de terminales utilizado.
   b. El detalle de transacciones permitidas por terminal.

5.2. Identificación y Autenticación de los Usuarios

1. Cada uno de los usuarios ya sea
   a. Personal de soporte técnico
   b. Operadores
   c. Administradores de red
   d. Programadores de sistemas
   e. Administradores de bases de datos)

Deberán tener un identificador único de usuario tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades

puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

2. En circunstancias excepcionales, cuando existe un claro beneficio para la Institución, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

5.3. Sistema de Administración de Contraseñas

La contraseña es el principal medio para la validación de un usuario para acceder al servicio informático.

El sistema de administración de contraseñas debe:

1. Dar contraseñas únicas para establecer responsabilidades.
2. Admitir que los usuarios escojan y cambien sus propias contraseñas y tener un control de verificación para contemplar los errores de ingreso.
3. Exigir a los usuarios a cambiar las contraseñas temporales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
4. Registrar las últimas contraseñas usadas por el usuario, y no permitir la reutilización de las mismas.
5. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

6. Guardar en forma independiente los archivos de contraseñas y los datos de sistemas de aplicación.

5.4. Uso de Utilitarios de Sistema

En su mayoría los sistemas informáticas deben usar varios utilitarios los cuales podrían pasar por alto los controles, por tal motivo es necesario que su uso sea limitado y minuciosamente controlado.

1. Se debe utilizar un control de autenticación para los usuarios de estos utilitarios.
2. Separar entre utilitarios del sistema y software de aplicaciones.
3. Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
4. Registrar todo uso de utilitarios del sistema.
5. Definir y documentar los niveles de autorización para utilitarios del sistema.

5.7. Desconexión de Terminales por Tiempo Muerto

1. El Responsable de Seguridad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la Institución, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto,

para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

2. Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.
3. Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

5.8. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la Institución.

Entre los controles que se deben aplicar, se enuncian:

1. Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

2. Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

6. CONTROL DE ACCESO A LAS APLICACIONES

Ilustración 27: Diseño de políticas de control de acceso a las aplicaciones

Elaboración: Investigadora

Fuente: Investigadora

1. Las aplicaciones se diseñarán con funciones de acceso para cada usuario del entorno operativo de la aplicación.

2. Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

3. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

4. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

7. MONITOREO DEL ACCESO Y USO DEL SISTEMA

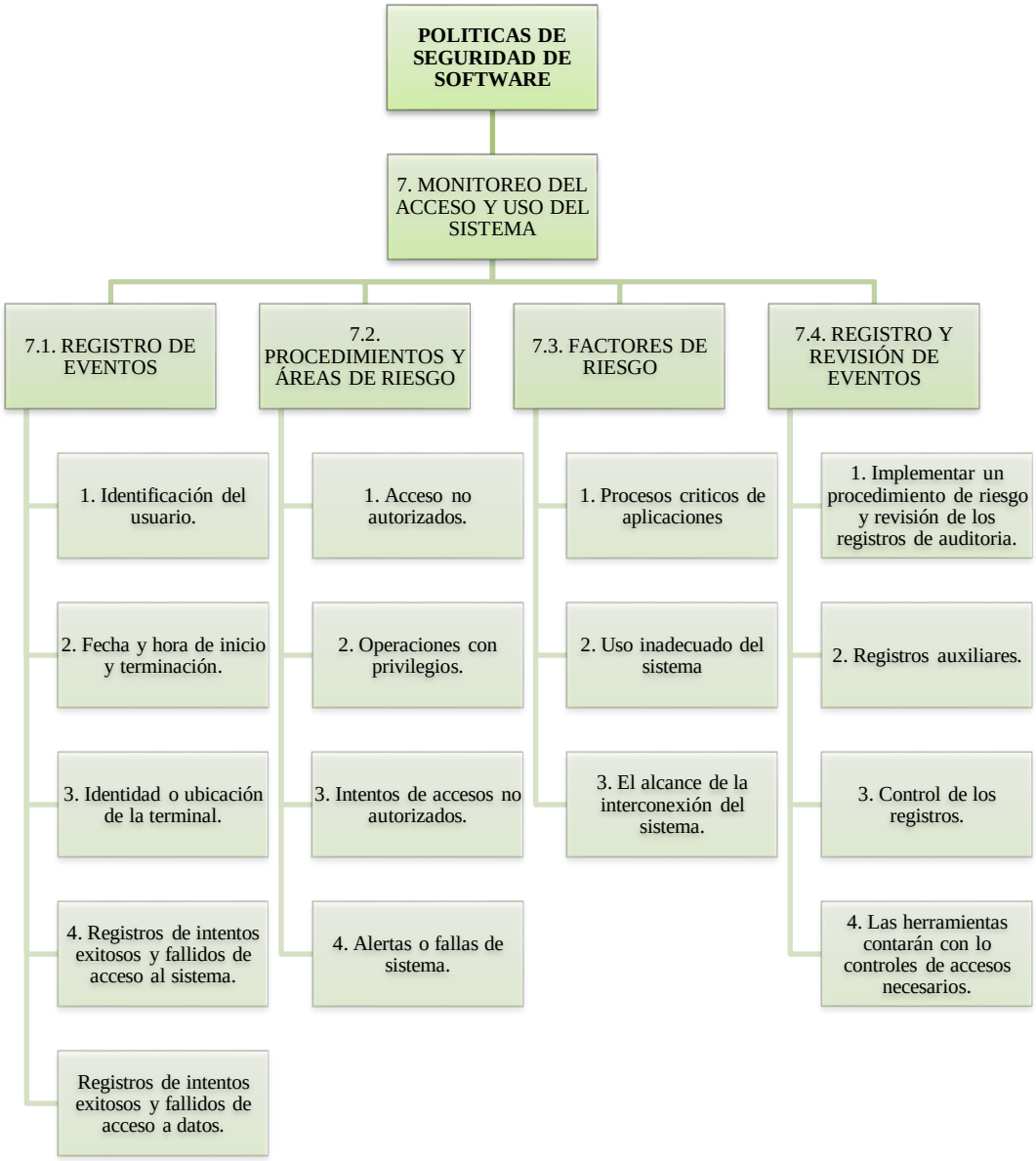

Ilustración 28: Diseño de políticas de monitoreo de acceso y uso del sistema

Elaboración: Investigadora

Fuente: Investigadora

7.1. Registro de Eventos

Deben generarse registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere.

Los registros de auditoría deberán incluir:

1. Identificación del usuario.
2. Fecha y hora de inicio y terminación de dicho evento.
3. Ubicación de la terminal en la que se generó el evento
4. Registros de intentos exitosos y fallidos de acceso al sistema.
5. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

7.2. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

1. Acceso no autorizado, incluyendo detalles como:
    a. Identificación del usuario.
    b. Fecha y hora de eventos clave.
    c. Tipos de eventos.
    d. Archivos a los que se accede.
    e. Utilitarios y programas utilizados.
2. Todas las operaciones con privilegio, como:
    a. Utilización de cuenta de supervisor.
    b. Inicio y cierre del sistema.
    c. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
    d. Cambio de fecha/hora.
    e. Cambios en la configuración de la seguridad.
    f. Alta de servicios.
3. Intentos de acceso no autorizado, como:
    a. Intentos fallidos.
    b. Violaciones de la Política de Accesos y notificaciones para “gateways” de red y “firewalls”.
    c. Alertas de sistemas de detección de intrusiones.
4. Alertas o fallas de sistema como:
    a. Alertas o mensajes de consola.

b. Excepciones del sistema de registro.

c. Alarmas del sistema de administración de redes.

d. Accesos remotos a los sistemas.

7.3. Factores de Riesgo

Entre los factores de riesgo que se deben considerar se encuentran:

1. La criticidad de los procesos de aplicaciones.
2. La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
3. El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

7.4. Registro y Revisión de Eventos

1. Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La periodicidad de dichas revisiones

será definida por los Propietarios de la Información y el Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

2. Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.
3. Por otra parte, el Responsable del Área Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.
4. Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

    a. La desactivación de la herramienta de registro.
    b. La alteración de mensajes registrados.
    c. La edición o supresión de archivos de registro.
    d. La saturación de un medio de soporte de archivos de registro.
    e. La falla en los registros de los eventos.
    f. La sobre escritura de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de

colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

8. GESTIÓN DE OPERACIONES Y COMUNICACIONES

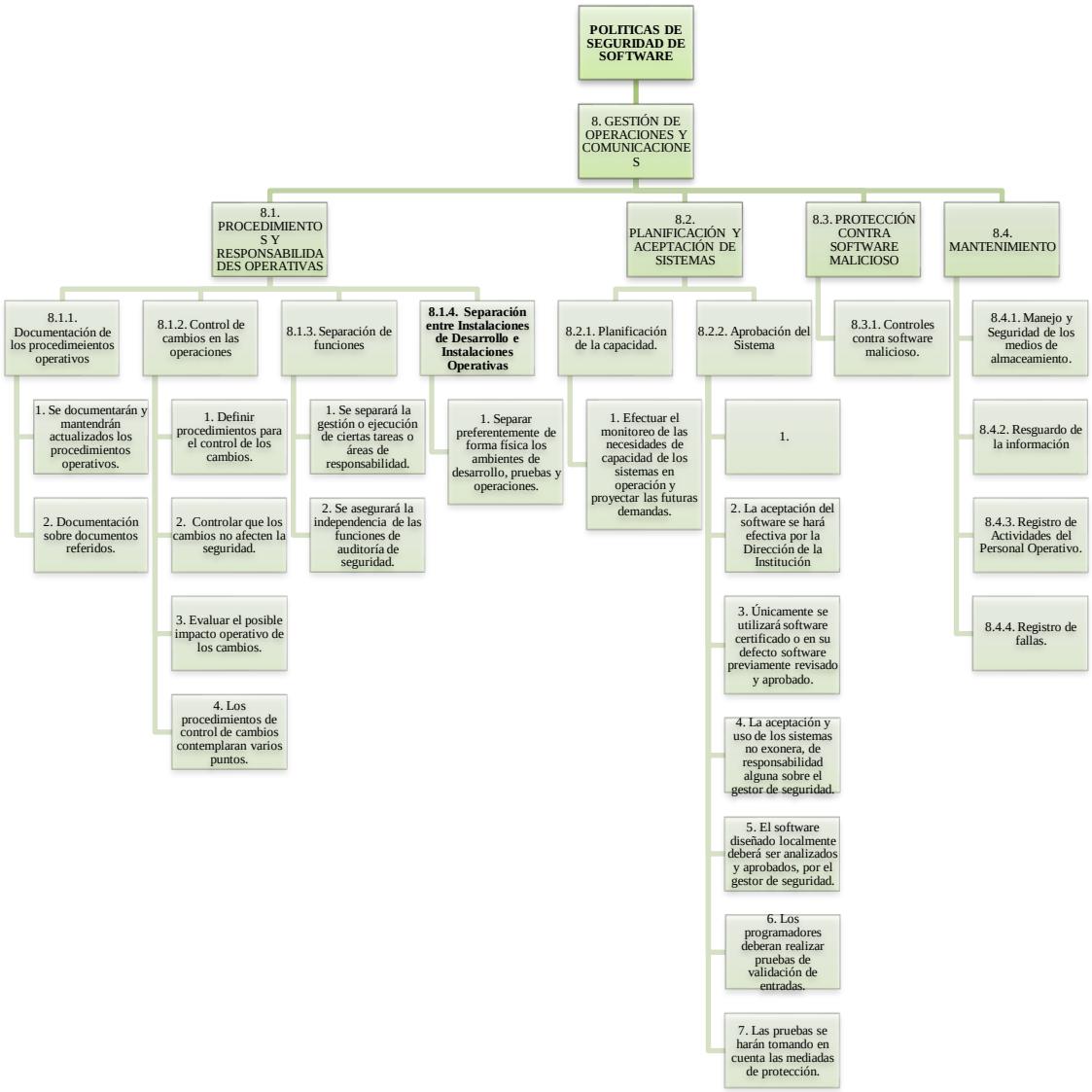

Ilustración 29: Diseño de políticas de operaciones y comunicaciones

Elaboración: Investigadora

Fuente: Investigadora

Generalidades

La proliferación de software malicioso, como virus, troyano, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas. Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre si, tanto dentro de la Institución como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivos

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Documentación de los Procedimientos Operativos

1. Se registraran y actualizaran los procesos operativos sus cambios serán autorizados por el Responsable de Seguridad Informática.

   Los procesos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

   a. Proceso y manejo de la información.
   b. Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
   c. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
   d. Restricciones en el uso de utilitarios del sistema.
   e. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

f. Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
g. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

2. Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a. Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
b. Instalación y mantenimiento de las plataformas de procesamiento.
c. Monitoreo del procesamiento y las comunicaciones.
d. Inicio y finalización de la ejecución de los sistemas.
e. Programación y ejecución de procesos.
f. Gestión de servicios.
g. Resguardo de información.
h. Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
i. Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

j. Uso del correo electrónico.

8.1.2. Control de Cambios en las Operaciones

1. Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.
2. El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.
3. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.
4. Los procedimientos de control de cambios contemplarán los siguientes puntos:
    a. Identificación y registro de cambios significativos.
    b. Evaluación del posible impacto de dichos cambios.
    c. Aprobación formal de los cambios propuestos.
    d. Planificación del proceso de cambio.
    e. Prueba del nuevo escenario.
    f. Comunicación de detalles de cambios a todas las personas pertinentes.
    g. Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

8.1.3. Separación de Funciones

1. Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

   Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

   a) Monitoreo de las actividades.
   b) Registros de auditoría y control periódico de los mismos.
   c) Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

2. Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

8.1.4. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

1. Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

   Para ello, se tendrán en cuenta los siguientes controles:

   a. Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
   b. Separar las actividades de desarrollo y prueba, en entornos diferentes.
   c. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.

d. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e. Definir propietarios de la información para cada un de los ambientes de procesamiento existentes.
f. El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

8.2 PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

8.2.1. Planificación de la Capacidad

1. El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada

componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

1. La unidad de informática, o personal de la misma dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la CISC.
2. La aceptación del software se hará efectiva por la Gerencia de la institución, previo análisis y pruebas efectuadas por el personal de informática.
3. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.
4. La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de los mismos.
5. El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación.

6. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:
    a. Valores fuera de rango.
    b. Caracteres inválidos, en los campos de datos.
    c. Datos incompletos.
    d. Datos con longitud excedente o valor fuera de rango.
    e. Datos no autorizados o inconsistentes.
    f. Procedimientos operativos de validación de errores
    g. Procedimientos operativos para validación de caracteres.
    h. Procedimientos operativos para validación de la integridad de los datos.
    i. Procedimientos operativos para validación e integridad de las salidas.
7. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

8.3 Protección contra software malicioso

8.3.1. Controles Contra Software Malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

1. Prohibir el uso de software no autorizado por la Institución
2. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
3. Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
4. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Institución, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

7. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
8. Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

8.4. Mantenimiento

1. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal de la unidad de informática, o del personal de soporte técnico.
2. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.
3. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

8.4.1. Manejo y seguridad de medios de almacenamiento

1. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

2. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.
3. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente, el gestor de seguridad o la gerencia administrativa, esta caja no debería ser removible, una segunda copia será resguardada por un tercero, entidad financiera o afín.
4. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

8.4.2. Resguardo de la Información

El Responsable del Área Informática y el de Seguridad Informática junto al Responsable del Área Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Institución, según el punto “Ensayo,

Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo.” de esta política.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

1. Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
2. Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
3. Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software Gestión deesenciales para la Institución. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.

4. Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
5. Probar periódicamente los medios de resguardo.
6. Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

8.4.3. Registro de Actividades del Personal Operativo

El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

1. Tiempos de inicio y cierre del sistema.
2. Errores del sistema y medidas correctivas tomadas.
3. Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
4. Ejecución de operaciones críticas
5. Cambios a información crítica

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

8.4.4. Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

1. Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
2. Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
3. Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

9. DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar

una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Institución en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Área de Sistemas, los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad Informática cumplirá las siguientes funciones:

- ✓ Definir los procedimientos de administración de claves.
- ✓ Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- ✓ Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- ✓ Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de su área que considere

adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

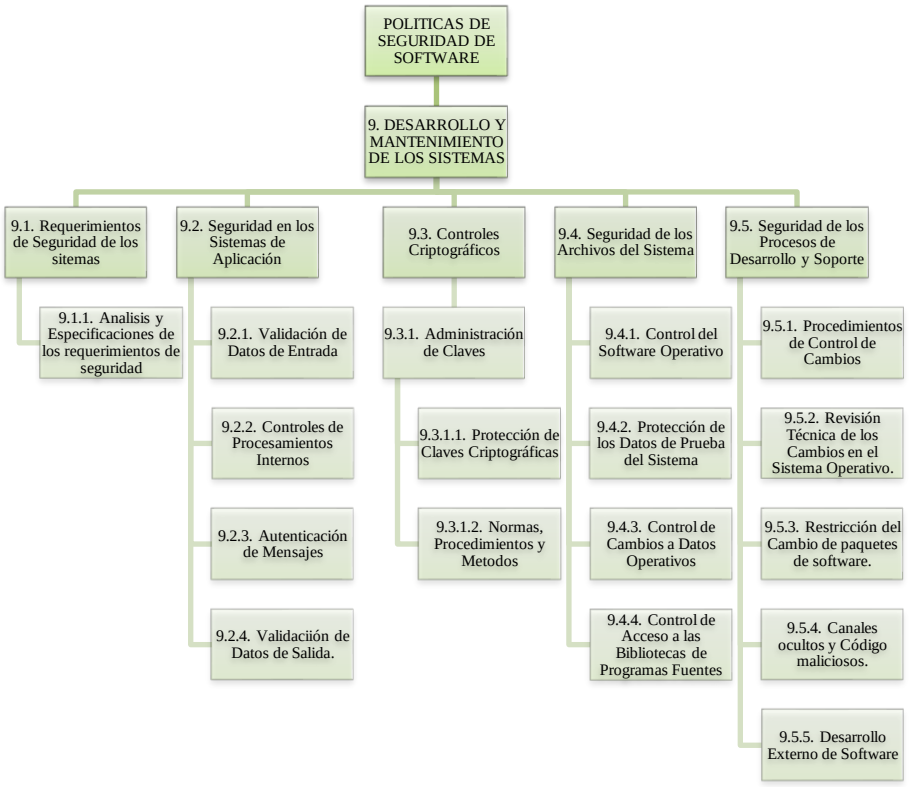

Ilustración 30: Diseño de la política de desarrollo y mantenimiento de los sistemas

9.1. Requerimientos de Seguridad de los Sistemas

9.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

1. Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema

2. Y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

3. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

4. Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

9.2. Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

1. La validación de datos de entrada.
2. El procesamiento interno.
3. La autenticación de mensajes (interfases entre sistemas)
4. La validación de datos de salida.

9.2.1. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

1. Control de secuencia.
2. Control de monto límite por operación y tipo de usuario.
3. Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
4. Control de paridad.
5. Control contra valores cargados en las tablas de datos.
6. Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

1. Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
2. Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.

3. Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

9.2.2. Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

1. Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
2. Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
3. Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
4. Procedimientos que realicen la validación de los datos generados por el sistema.

5. Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
6. Procedimientos que controlen la integridad de registros y archivos.
7. Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
8. Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

9.2.3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto “Controles Criptográficos”.

9.2.4. Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

1. Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
2. Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

3. Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
4. Procedimientos para responder a las pruebas de validación de salidas.
5. Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

9.3. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

9.3.1. Administración de Claves

9.3.1.1.Protección de Claves Criptográficas

1. Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte de la Institución de los dos tipos de técnicas criptográficas, a saber:

a. Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.
b. Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

2. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

9.3.1.2.Normas, Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

1. Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
2. Generar y obtener certificados de clave pública de manera segura.
3. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

4. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
5. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
6. Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deben archivarse).
7. Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades de la Institución, por ejemplo para la recuperación de la información cifrada.
8. Archivar claves, por ejemplo, para la información archivada o resguardada.
9. Destruir claves.
10. Registrar y auditar las actividades relativas a la administración de claves.

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso es llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

9.4. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

9.4.1. Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

1. Toda aplicación, desarrollada por la Institución o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática.
2. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
3. El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:

    a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

1. Guardar sólo los ejecutables en el ambiente de producción.
2. Llevar un registro de auditoría de las actualizaciones realizadas.
3. Retener las versiones previas del sistema, como medida de contingencia.
4. Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
5. Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
6. Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

9.4.2. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

1. Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
2. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
3. Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

9.4.3. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad Informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

1. Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
2. El Propietario de la Información afectada y del Responsable de Seguridad Informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
3. Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
4. Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo.
5. Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad Informática.

9.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

1. El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:

    a. Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
    b. Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
    c. Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
    d. Administrar las distintas versiones de una aplicación.

e. Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

2. Denegar al “administrador de programas fuentes” permisos de modificación sobre los programas fuentes bajo su custodia.
3. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
4. Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
5. Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
6. Evitar que la función de “administrador de programas fuentes” sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
7. Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
8. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

9. Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la Institución en los procedimientos que surgen de la presente política.

9.5. Seguridad de los Procesos de Desarrollo y Soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

9.5.1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

1. Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
2. Mantener un registro de los niveles de autorización acordados.

3. Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
4. Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
5. Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
6. Obtener aprobación formal por parte del Responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.
7. Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
8. Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
9. Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
10. Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
11. Mantener un control de versiones para todas las actualizaciones de software.
12. Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
13. Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

14. Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en “Control del Software Operativo”.

9.5.2. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

1. Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
2. Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
3. Asegurar la actualización del Plan de Continuidad de las Actividades de la Institución.

9.5.3. Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

1. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
2. Determinar la conveniencia de que la modificación sea efectuada por la Institución, por el proveedor o por un tercero.
3. Evaluar el impacto que se produce si la Institución se hace cargo del mantenimiento.
4. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

9.5.4. Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

1. Adquirir programas a proveedores acreditados o productos ya evaluados.
2. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
3. Controlar el acceso y las modificaciones al código instalado.
4. Utilizar herramientas para la protección contra la infección del software con código malicioso.

9.5.5. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

1. Acuerdos de licencias, propiedad de código y derechos conferidos.
2. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
3. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
4. Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

SEGURIDAD ORGANIZACIONAL

EN CUANTO A POLÍTICAS GENERALES DE SEGURIDAD

Unidad de Informática:

1. El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional.

2. El administrador hará respaldos periódicos de la información así como la depuración de los discos duros.
3. El gestor de seguridad, junto al administrador de sistemas, realizarán auditorias periódicas en el sistema con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos de un servidor.
4. El administrador decidirá, sobre el uso de los recursos del sistema restricción de directorios y programas ejecutables para los usuarios.
5. Se revisará el tráfico de paquetes que se estén generando dentro de un segmento de red, a fin de determinar si se está haciendo mal uso de la red o se esta generando algún problema que pueda llevar a que se colapsen los sistemas.
6. El administrador de sistemas, dará de alta y baja a usuarios y revisará las cuentas periódicamente para estar seguros de que no hay usuarios ficticios.
7. Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red
8. Reportar a las autoridades universitarias, las fallas en el desempeño de la red. Solucionar junto al gestor de seguridad, los problemas que se generen en su red local.
9. La universidad se guarda el derecho de divulgación o confidencialidad de la información personal de los usuarios de la red institucional, si estos se ven envueltos en actos ilícitos.

10. El gestor de seguridad monitoreara las acciones y tareas de los usuarios de la red institucional.
11. Se prestará el servicio de Internet, siempre que se encuentren presentes los requisitos de seguridad mínimos.
12. El usuario no tiene derecho sobre el servicio de Internet sino es mediante la aceptación de la normativa de seguridad.
13. Se suspenderá cualquier usuario que utilice los centros de cómputo fuera del ámbito académico, y los objetivos para los que estos fueron creados.

EXCEPCIONES DE RESPONSABILIDAD

1. La institución debe establecer con sus empleados un contrato de confidencialidad de común acuerdo.
2. Toda acción debe seguir los canales de gestión necesarios para su ejecución.
3. El comité de seguridad proveerá la documentación necesaria para aprobar un acuerdo de no responsabilidad por acciones que realicen dentro de la red institucional.
4. Las gestiones para las excepciones de responsabilidad son acordadas bajo común acuerdo de la gerencia y el comité de seguridad.

CLASIFICACIÓN Y CONTROL DE ACTIVOS

RESPONSABILIDAD POR LOS ACTIVOS

1. El comité de seguridad nombrará un responsable de activos en cada departamento de la Universidad.
2. Los jefes de cada departamento de la institución, son responsables de mantener o proteger los activos de mayor importancia.

CLASIFICACIÓN DE LA INFORMACION

1. Cada jefe de departamento dará importancia a la información en base al nivel de clasificación que demande el activo.
2. La información pública puede ser visualizada por cualquier persona dentro o fuera de la institución.
3. La información interna, es propiedad del estudiante y de la institución, en ningún momento intervendrán personas ajenas a su proceso o manipulación.
4. La información confidencial es propiedad absoluta de la institución, el acceso a ésta es permitido únicamente a personal administrativo.
5. Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

SEGURIDAD LIGADA AL PERSONAL

Referente a contratos.

1. Todo empleado ejercerá las labores estipuladas en su contrato de trabajo.
2. El empleado.
3. El empleado no tiene ningún derecho sobre la información que procese dentro de las instalaciones de la red institucional.
4. La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito de laboral.
5. El usuario se norma por las disposiciones de seguridad informática de la Universidad.
6. Los usuarios son responsables de las acciones causadas por sus operaciones con el equipo de la red institucional.

CAPACITACIÓN DE USUARIOS

1. El comité de seguridad capacitará los usuarios de la red institucional, por departamentos.
2. El comité de seguridad proporcionara las fechas en que se impartirán las capacitaciones.

3. El material de apoyo (manuales, guías, etc.) será entregado minutos antes de iniciar la capacitación, en la sala donde será efectuada la capacitación.
4. En cada capacitación se revisarán los dispositivos de conexión de servicios involucrados en la capacitación.
5. Las capacitaciones deben realizarse fuera de áreas de procesamiento de información.
6. Entre los deberes y derechos de los empleados institucionales y personal denotado como tercero, se encuentran acatar o respetar las disposiciones sobre capacitaciones y por ende asistir a ellas sin excepción alguna, salvo casos especiales.

RESPUESTA A INCIDENTES Y ANOMALIAS DE SEGURIDAD

1. Los respaldos de información deberán ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la institución.
2. Los respaldos se utilizarán únicamente en casos especiales ya que su contenido es de suma importancia para la institución.
3. La institución debe contar con respaldos de la información ante cualquier incidente.
4. Generar procedimientos manuales de respaldo de información

5. La unidad de informática tendrá la responsabilidad, de priorizar una situación de la otra en cuanto a los problemas en las estaciones de trabajo.
6. En situaciones de emergencia que impliquen áreas como atención al cliente entre otros, se da prioridad en el orden siguiente.
    a. Área de contabilidad
    b. Área académica
    c. Área administrativa.
7. El documento de seguridad se elaborará, tomando en cuenta aspectos basados en situaciones pasadas, y enmarcarlo en la pro actividad de situaciones futuras.
8. Se prioriza la información de mayor importancia para la institución.
9. Se evacua la información o activo de los niveles confidenciales de la institución.
10. Respaldar los archivos de logs o registro de los sistemas en proceso, cada cierto tiempo durante el día.
11. Llevar un registro manual de las actividades sospechosas de los empleados

PROCEDIMIENTOS DE LA INVESTIGACIÓN

El problema:

Planteamiento del problema

Causas y consecuencias del problema

Delimitación, Formulación y Evaluación de problema

Objetivos de la Investigación

Justificación e Importancia de la investigación

Marco teórico:

Antecedentes

Fundamentación teórica

Fundamentación legal

Preguntas a contestarse

Definición de variables

Definiciones conceptuales

Metodología:

Diseño de Investigación (Modalidad y Tipo de Investigación)

Población y Muestra

Operación de variables, dimensiones e indicadores

Instrumentos de recolección de datos

Procedimiento de la Investigación

Procesamiento y Análisis

Análisis de Situación Actual - Análisis de Riesgo

Criterios para la elaboración de la propuesta

Criterios para la validación de la propuesta

Marco Administrativo:

Cronograma

Presupuesto

Referencias Bibliográficas

Anexos

CRITERIOS PARA LA ELABORACIÓN DE LA PROPUESTA

Uno de los principales motivos por el cual se realiza este proyecto es porque se desea realizar un diseño adecuado de la seguridad informática en software con el cual se pretende disminuir el riesgo de vulnerabilidad encontrada en el departamento técnico informático de la CISC.

El diseño se lo elaborará en base a estudios ya realizados, en los cuales se ha tomado en cuenta procedimientos, normas, políticas y estándares sobre controles de seguridad informática en software que nos garantizaran una mejor calidad sobre seguridad para nuestra institución.

Los puntos que se tomaron en cuenta para la elaboración del diseño son:

1. Control de Accesos
2. Administración del Acceso de Usuarios
3. Seguridad en Acceso de Terceros
4. Control de Acceso a la Red
5. Control de Acceso a los Sistemas Operativos
6. Control de Acceso a las Aplicaciones
7. Monitoreo del Acceso y Uso del Sistema
8. Gestión de operaciones y comunicaciones
9. Desarrollo y Mantenimiento de los Sistemas

CRITERIOS DE VALIDACIÓN DE LA PROPUESTA

La estrategia utilizada para la elaboración de esta propuesta es en base a juicio de expertos, estudios sobre seguridad informática ya realizados en otras instituciones, información recogida en estándares establecidos como Itil, Cobit, Iso.

CAPÍTULO IV

MARCO ADMINISTRATIVO

CRONOGRAMA

NOMBRE DE LA TAREA	DURACIÓN	COMIENZO	FIN
ANALISIS Y DISEÑO DE LA SEGURIDAD EN SOFTWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y NETWORKING	167 días	21/04/2010	30/11/2010
CHARLAS, ORIENTACIÓN Y ENTREGA DEL TEMA DE TESIS	48 días	21/04/2010	25/06/2010
Charlas del 2do Seminario de Fin de Carrera	21 días	21/04/2010	19/05/2010
Elaboración del Tema de Tesis	15 días	20/05/2010	09/06/2010
Elaboración de Objetivos Generales y Objetivos Específicos	15 días	20/05/2010	09/06/2010
Elaboración del Planteamiento del problema	15 días	20/05/2010	09/06/2010
Elaboración de los Alcances	15 días	20/05/2010	09/06/2010
Presentación de la Propuesta de Tesis al Dpto. de Graduación de la Carrera	1 día	26/05/2010	26/05/2010
Proceso de revisión y aprobación del tema propuesto por parte del Dpto. de Graduación	22 días	27/05/2010	25/06/2010
PROCESO DE TUTORIAS	118 días	28/06/2010	29/11/2010
CONSTRUCCIÓN Y CORRECCION DEL CAPITULO I	23 días	28/06/2010	27/07/2010
Revisión y Corrección del Tema de Tesis	10 días	28/06/2010	08/07/2010

NOMBRE DE LA TAREA	DURACIÓN	COMIENZO	FIN
Revisión y Corrección de Introducción	10 días	09/07/2010	22/07/2010
Revisión y Corrección de Objetivos Generales	10 días	09/07/2010	22/07/2010
Revisión y Corrección de Objetivos Específicos	10 días	09/07/2010	22/07/2010
Revisión y Corrección de Introducción	10 días	09/07/2010	22/07/2010
Elaboración de la Descripción del Problema	10 días	09/07/2010	22/07/2010
Revisión y Corrección de Alcances	10 días	09/07/2010	22/07/2010
Solicitud de permisos para realizar el levantamiento de información del Departamento Técnico Informático de la CISC	3 días	23/07/2010	27/07/2010
CONSTRUCCIÓN Y CORRECCIÓN DEL CAPITULO II	11 días	28/07/2010	09/08/2010
Investigación de Información sobre el tema	11 días	28/07/2010	09/08/2010
Selección de información relevante del tema	5 días	28/07/2010	03/08/2010
Investigación de Información de temas relacionados	1 día	04/08/2010	04/08/2010
Elaboración del Marco Teórico	5 días	05/08/2010	09/08/2010
CONSTRUCCIÓN Y CORRECCIÓN DEL CAPITULO III	58 días	09/08/2010	21/10/2010
ANALISIS DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CISC	25 días	09/08/2010	08/09/2010
Elaboración de Entrevistas para el Administrador del Departamento Técnico Informático de la CISC	5 días	09/08/2010	13/08/2010
Levantamiento de Información del Departamento Técnico Informático de la CISC	3 días	16/08/2010	18/08/2010
Elaboración del análisis de las entrevistas realizadas	15 días	19/08/2010	07/09/2010
Investigación de Temas de Seguridad Informática en Software	5 días	02/09/2010	08/09/2010
DISEÑO DE LA SEGURIDAD EN SOFTWARE	24 días	22/09/2010	21/10/2010
Elaboración de Políticas de Seguridad en Software	15 días	22/09/2010	08/10/2010

NOMBRE DE LA TAREA	DURACIÓN	COMIENZO	FIN
Elaboración del Diseño de la Seguridad Informática en Software para el Departamento Técnico Informático de la CISC	15 días	01/10/2010	21/10/2010
Presentación de avances	1 día	15/10/2010	15/10/2010
Corrección de avances	5 días	15/10/2010	21/10/2010
CONSTRUCCIÓN Y CORRECCIÓN DEL CAPITULO IV	11 días	22/10/2010	05/11/2010
Elaboración del Capítulo IV	5 días	22/10/2010	28/10/2010
Presentación de avances	1 día	29/10/2010	29/10/2010
Corrección de avances	5 días	01/11/2010	05/11/2010
CONSTRUCCIÓN Y CORRECCIÓN DEL CAPITULO V	16 días	08/11/2010	29/11/2010
Elaboración de las Conclusiones	5 días	08/11/2010	12/11/2010
Elaboración de las Recomendaciones	5 días	08/11/2010	12/11/2010
Presentación de avances	1 día	15/11/2010	15/11/2010
Correccion de Avances	10 días	16/11/2010	29/11/2010
ENTREGA FINAL DE LA TESIS	1 día	30/11/2010	30/11/2010

PRESUPUESTO

Detalle de los egresos del proyecto

Detalle de los egresos del proyecto comprendido entre los meses de Junio – Diciembre

EGRESOS		**DÓLARES**
Suministros de oficina y computación	$	5.00
Servicios de Internet		34.16
Transporte		20.00
Alimentación		23.00
Impresión		5.00
Servicios básicos (Energía Eléctrica)		10.00
SUB-TOTAL……..…	$	**97.16**
TOTAL MESES JUNIO – DICIEMBRE…...	**$**	**582.96**

Detalle de los egresos del proyecto del mes de Enero

EGRESOS	DÓLARES
Suministros de oficina y computación	$ 15.00
Servicios de Internet	34.16
Transporte	20.00
Alimentación	23.00
Impresión primer borrador	70.00
Impresión segundo borrador	70.00
Servicios básicos (Luz)	3.00
Impresión de Originales	70.00
Empaste de la tesis	60.00
SUB-TOTAL……	$ **265.16**

PRESUPUESTO TOTAL DEL PROYECTO

EGRESOS	DÓLARES
Computadora	$ 500.00
Total gastos meses de Abril - Diciembre	582.96
Total gastos mes de Enero	295.16
TOTAL……	$ **1,448.12**

BIBLIOGRAFÍA

DIRECCIONES WEB

ALEGSA.com.ar. (s.f.). Recuperado el 1 de Octubre de 2010, de http://www.alegsa.com.ar/Dic/servidor%20de%20aplicaciones.php

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/identificacion.htm

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/seguridadlogica.htm

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/acceso.htm

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/accesointerno.htm

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/accesoexterno.htm

Borghello, C. F. (s.f.). *SEGU-INFO Seguridad de la Información*. Recuperado el 24 de Agosto de 2010, de http://www.segu-info.com.ar/logica/administracion.htm

Flores, C. H. (11 de Enero de 2010). *Configuración del Centro de Computo*. Recuperado el 8 de Agosto de 2010, de http://cesarhernandezflores.blogspot.com/

Jaime, J. (29 de Abril de 2009). *ISSUU*. Recuperado el 29 de Septiembre de 2010, de http://issuu.com/jjaime/docs/windows_xp_hardening

Martinez, R. (s.f.). *www.linux-es.org*. Recuperado el 27 de Septiembre de 2010, de El rincon de linux para Hispanohablantes: http://www.linux-es.org/kernel

Modelo de Política de la Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. (Julio de 2005). Recuperado el 15 de Octubre de 2010, de http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

Paz, A. (29 de Enero de 2008). *Guru de la Informatica*. Recuperado el 27 de Septiembre de 2010, de Hardening Linux: http://vtroger.blogspot.com/2008/01/hardening-linux-con-grsecurity.html

RED, R. (Noviembre de 2002). *CiberHabitat, Ciudad de la Informatica*. Recuperado el 08 de Agosto de 2010, de http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm

Redes Tecnológicas. (26 de Junio de 2008). Recuperado el 1 de Octubre de 2010, de http://redesadsi.wordpress.com/2008/06/26/redes-tecnologicas/

Rutinel, J. U. (1997). *Diccionarios de Investigación Científica.* Santo Domingo, República Dominicana: Editora Universitaria UASD (Univesidad Autonoma de Santo Domingo).

Sabino, C. (1978). *El proceso de la investigación.* Buenos Aires, Argentina: Editorial El Cid Editor.

SCRBD. (2 de Enero de 2008). Recuperado el 8 de Octubre de 2010, de http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica

Tanys. (20 de Mayo de 2009). *Tanys*. Recuperado el 28 de Octubre de 2010, de http://blackdahlie.blogspot.com/2009/05/hablemoss-de-servidores-dns-y-dhcp.html

WIKIPEDIA La enciclopedia libre. (23 de Noviembre de 2009). Recuperado el 5 de Septiembre de 2010, de http://es.wikipedia.org/wiki/Portal_Cautivo

WIKIPEDIA la enciclopedia libre. (Julio de 2010). Recuperado el 24 de Agosto de 2010, de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

WIKIPEDIA La enciclopedia libre. (1 de Septiembre de 2010). Recuperado el 5 de Septiembre de 2010, de http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

WIKIPEDIA La enciclopedia libre. (2 de Septiembre de 2010). Recuperado el 5 de Septiembre de 2010, de http://es.wikipedia.org/wiki/Proxy

WIKIPEDIA La enciclopedia libre. (2 de Septiembre de 2010). Recuperado el 5 de Septiembre de 2010, de http://es.wikipedia.org/wiki/Proxy

WIKIPEDIA La enciclopedia libre. (17 de Agosto de 2010). Recuperado el 5 de Septiembre de 2010, de http://es.wikipedia.org/wiki/DHCP

WIKIPEDIA La enciclopedia libre. (22 de Junio de 2010). Recuperado el 6 de Septiembre de 2010, de http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

yabembre. (22 de Marzo de 2006). Recuperado el 1 de Octubre de 2010, de http://yabrembre.blogspot.com/2006/03/las-x-windows-i.html

ANEXOS

ENTREVISTA QUE SE REALIZÓ AL PERSONAL DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES Y NETWORKING

1. **¿Cuántas áreas posee el Dpto. Tecnológico?**

   Área de hardware _____

   Área de software _____

   Área de programación _____

   Soporte técnico (Ayudantes de hardware) _____

2. **¿Cuántas personas tienen acceso al Dpto. Tecnológico?**

   Administradores _____

   Pasantes _____

   Otros _____

3. **Existe algún software o propiedad del sistema operativo registre el acceso de los usuarios a los servidores (Nombre del usuario, fecha, hora, modificaciones, etc.)**

4. **Bajo que parámetros realizan la selección de hardware y software (Estudios, investigaciones, precios, calidad, etc.)**

Se realiza estudios, se solicitan los equipos pero no todo es adquirido sino más bien trabajan con los recursos que tienen.

5. Numero de servidores y funciones de cada uno

(2 Servidores, 6 máquinas personales adaptadas para servidor)

2 Servidores Bases de Datos (Administrativa y Alumnos)

1 Servidor de información

2 Servidores Firewall (Laboratorio 1,2 y Laboratorio 3,4,5)

1 Servidor Web

1 Servidor de Correo

1 Firewall Principal

<u>En cuanto a recurso humano:</u>

6. ¿Se recibe formación y se planifica ésta mediante asistencia a cursos, seminarios,etc.?

Si

No

Si es No explique porque _____

_____

7. ¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas?

SÍ ( ) NO ( )

8. ¿Se solicitan demostraciones sobre los nuevos artículos a los proveedores?

SÍ ( ) NO ( )

9. ¿La entidad dispone de un plan informático?

SÍ ( ) NO ( )

10. ¿Se están siguiendo las directrices marcadas por el plan?

SÍ ( ) NO ( )

<u>En Cuanto a Gestión de Proyectos</u>

11. ¿Quién autoriza los proyectos?

Nombre:

Cargo que desempeña:

12. ¿Cómo se asignan los recursos? Humano, económicos, software.

13. ¿Cómo se estiman los tiempos de duración?

14. ¿Quién interviene en la planeación de los proyectos?

15. ¿Cómo se calcula el presupuesto del proyecto?

16. ¿Qué técnicas se usan en el control de los proyectos?

17. ¿Quién asigna las prioridades?

18. ¿Cómo se asignan las prioridades?

19. ¿Cómo se controla el avance del proyecto?

20. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?

21. ¿Cómo se estima el rendimiento del personal?

22. ¿Quiénes intervienen al diseñar un sistema?

( ) Usuario.

( ) Analista.

( ) Programadores.

( ) Operadores.

( ) Gerente de departamento.

( ) Auditores internos.

( ) Asesores.

( ) Otros.

23. ¿Los analistas son también programadores?

SÍ ( ) NO ( )

24. ¿Qué lenguaje o lenguajes conocen los analistas?

25. ¿Cuántos analistas hay y qué experiencia tienen?

26. ¿Qué lenguaje conocen los programadores?

27. ¿Cómo se controla el trabajo de los analistas?

28. ¿Cómo se controla el trabajo de los programadores?

29. ¿Qué documentación acompaña al programa cuando se entrega?

<u>En cuanto a dispositivos de almacenamiento:</u>

30. ¿Se tienen identificados los archivos con información confidencial y se cuenta conclaves de acceso?

SI ( ) NO ( )

¿Cómo lo identifican?_____ ____

31. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

32. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

Otro

(especifique)_____

33. Este almacén está situado:

En el mismo edificio del departamento ( )

En otro lugar ( )

¿Cual?_____

34. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechanestos?

SI ( ) NO ( )

35. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

36. ¿Se tiene un responsable, por turno, de los servidores de datos?

SI ( ) NO ( )

Solo se trabaja en el horario de: _____

37. ¿Se realizan auditorías periódicas a los medios de almacenamiento?

SI ( ) NO ( )

38. ¿Qué medidas se toman en el caso de extravío de algún dispositivo dealmacenamiento?

Si nunca se ha extraviado, ¿Qué medidas se tomarían de darse el caso?

39. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos dealmacenamiento?

SI ( ) NO ( )

40. ¿Se tiene relación del personal autorizado para firmar la salida de archivosconfidenciales?

SI ( ) NO ( )

41. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en quese devolverán?

SI ( ) NO ( )

42. ¿Se lleva control sobre los archivos prestados por el departamento?

SI ( ) NO ( )

43. En caso de préstamo ¿Conque información se documentan?

Nombre de la institución o usuario a quién se hace el préstamo.( )

Fecha de recepción ( )

Fecha en que se debe devolver ( )

Archivos que contiene ( )

Formatos ( )

Cifras de control ( )

Código de grabación ( )

Nombre del responsable que los presto ( )

Otros_____

44. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen losarchivos maestros

45. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

46. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

SI ( ) NO ( )

47. En los procesos que manejan archivos en línea, ¿Existen procedimientos pararecuperar los archivos?

SI ( ) NO ( )

48. ¿Estos procedimientos los conocen los operadores o administrador?

SI ( ) NO ( )

49. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL ( ) ANUAL ( ) SEMESTRAL ( ) OTRA ( )

50. ¿Existe un responsable en caso de falla?

SI ( ) NO ( )

51. ¿Explique qué políticas se siguen para la obtención de archivos de respaldo y a quienes se realizan estos respaldos?

52. ¿Existe un procedimiento para el manejo de la información del *cuarto frió*?

SI ( ) NO ( )

53. ¿Lo conoce y lo sigue el operador o administrador?

SI ( ) NO ( )

54. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programacióninformes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO ( )

¿Con qué frecuencia? _____

55. ¿Con que tipo de programas cuentan en los equipos de cómputo?

_____

_____

_____

_____

_____

56. ¿Cuentan con manuales para cadaprograma que se maneja?

SI ( ) NO ( )

57. ¿El personal sabe del contenido de estos manuales?

SI ( ) NO ( )

58. ¿Se cuenta con reglamento para el usuario, administrador y personal en general?

SI ( ) NO ( )

59. ¿Usuarios y maestros respetan los reglamentos y políticas estipuladas dentro del centro de cómputo?

SI ( ) NO ( )

60. ¿El reglamento está a la vista del usuario?

SI ( ) NO ( )

61. ¿Qué tipo de mantenimiento realizan?

a. Preventivo b.Correctivo

¿Por qué razón? _____

_____

62. ¿Qué materiales utilizan para realizar el mantenimiento de software?

63. ¿Tienen un lugar específico para guardar el material de mantenimiento de software?

SI ( ) NO ( )

64. ¿Los usuarios tienen la suficiente confianza como para presentar su queja sobre fallas en los equipos?

SI ( ) NO ( )

65. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

SI ( ) NO ( )

66. ¿Se tienen establecidos procedimientos de actualización a estas copias?

SI ( ) NO ( )

67. ¿Se ha establecido que información puede ser manipulada o no y por qué persona?

SI ( ) NO ( )

68. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?

SI ( ) NO ( )

69. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos?

SI ( ) NO ( )

70. ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?

Si_____

(¿Cuál?_____)

No_____ (¿Por qué?

_____)

71. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?

Si

(Descríbalo_____)

No_____

72. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?

SI ( ) NO ( )

73. ¿Se apega a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas?

SI ( ) NO ( )

El plan estratégico deberá establecer los servicios que se presentarán en un futuro:

74. ¿Cuáles servicios se implementarán?

75. ¿Cuándo se pondrán a disposición de los usuarios?

76. ¿Qué características tendrán?

77. ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

78. ¿Qué aplicaciones serán desarrolladas y cuándo?

79. ¿Qué tipo de archivos se utilizarán y cuándo?

80. ¿Qué bases de datos serán utilizarán y cuándo?

81. ¿Qué lenguajes se utilizarán y en que software?

82. ¿Qué tecnología será utilizada y cuando se implementará?

83. ¿Cuántos recursos se requerirán aproximadamente?

84. ¿Cuál es aproximadamente el monto de la inversión en software?

85. ¿Existen procedimientos formales para la operación del sistema decómputo?

SI () NO ( )

86. ¿Están actualizados los procedimientos?

SI ( ) NO ( )

87. Indique la periodicidad de la actualización de los procedimientos:

Semestral ( ) Anual ( )

Cada vez que haya cambio de equipo ( )

VALIDACIÓN DEL TEMA DE PROYECTO DE TESIS SEGÚN CRITERIO DE DOCENTES DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONES.

TEMA: ANÁLISIS Y DISEÑO DE LA SEGURIDAD DE SOFTWARE DEL DEPARTAMENTO TÉCNICO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

1. ¿Cree usted que es necesario reestructurar la seguridad del software en el departamento técnico informático de la carrera de ingeniería en sistemas computacionales?

   Si _____

   No _____

2. ¿Cada cuánto tiempo cree usted que debería evaluarse la seguridad de software dentro del departamento técnico informático de la CISC?.

   3 meses _____ 6 meses _____

   9 meses _____ 12 meses _____

3. ¿Cree usted que debería definirse en el departamento técnico un responsable de la seguridad de software?

   Si _____

   No _____

Por qué? : _____

_____

4. Para usted, ¿Cuál sería el nivel de importancia de este proyecto?.

   Bajo _____

   Medio _____

   Alto _____

5. Según su criterio, ¿Qué cree usted que debería tener un diseño de seguridad y en base a qué debería realizarse?

   _____

   _____

   _____

PREGUNTAS A CONTESTARSE

1. Qué funciones debería cumplir el Responsable de la seguridad informática de software?

   a. _____

   b. _____

   c. _____

2. ¿Cree usted que se debería realizar un análisis de seguridad y de procesos previo a la elaboración de un diseño de seguridad?

   SI _____

   NO _____

   POR QUE?

   _____

   _____

3. Según su criterio, ¿Qué controles se debe incluir en un diseño de seguridad informática de software?

   _____

   _____

   _____

4. ¿Qué tan importante es tener definidas políticas de seguridad en un centro de cómputo?

   Bajo _____

Medio _____

Alto _____

5. ¿Quiénes deben estar involucrados en cumplir con la seguridad informática en una institución educativa?

   Usuarios (estudiantes) _____

   Personal de sistemas _____

   Personal administrativo y docentes _____

   Otros (Indique quienes)

   _____

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

La seguridad informática se ha vuelto cada vez más necesaria a nivel de toda organización, a medida que pasa el tiempo hemos notado que los riesgos que sufren por causas de ataques es real y tienen un gran impacto a nivel de software, en muchas ocasiones las perdidas tienen un valor incalculable y no solo a nivel económico sino al flujo de información valiosa para la organización que puede existir por causas de estos ataques.

En la actualidad las organizaciones deben involucrarse y darles mayor importancia a nivel de seguridad que tienen implementado, ya que no se puede dejar ningún tipo de vulnerabilidad para que pueda acceder algún tipo de virus o ataque de intrusos, es decir debemos implementar más allá de firewall o cortafuegos, sistemas de detección de intrusos, antivirus, VPN, etc. si no que debemos estar seguros que estos tengan el funcionamiento adecuado y hacer que el personal tenga conocimientos y estén implicados en temas de seguridad.

No solo la tecnología aunque tiene un papel muy importante es necesaria para cubrir las vulnerabilidades que tiene la organización, si no debemos diseñar e implementar políticas y controles que permitan establecer una seguridad informática en software de calidad.

Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás, la seguridad tiene que formar parte de la organización y no debe basarse solo en los conocimientos con los que cuenta en personal si no se debe capacitar y actualizar a dicho personal para que estén preparados ante algún tema referente a seguridad.

Otro factor importante por lo que la seguridad informática en software no es un tema primordial en las organizaciones es el factor económico ya que los directivos no saben con exactitud qué es lo que se está resguardando o protegiendo o cuales serían las consecuencias de los posibles ataques a los que estamos expuestos y por este motivo no lo ven como un tema relevante en el cual se pueda invertir.

Debemos tener en cuenta que la seguridad total no existe o al menos no es posible cubrir todas las vulnerabilidades que tiene el centro de cómputo, sin embargo tomando en cuenta y poniendo en práctica determinadas reglas, estándares de seguridad informática en software podemos contrarrestar muchas de las anomalías que pueden existir.

En el presente trabajo se diseñaron diferentes tipos de políticas basándose en estudios ya realizados y en estándares internacionales como COBIT, ITIL, NORMAS ISO que nos servirán de guía para obtener mayor seguridad informática en software en la Carrera de Ingeniería en Sistemas Computacionales y NetWorking.

RECOMENDACIONES

Las recomendaciones se basan fundamentalmente en el análisis que es el resultado de las entrevistas que se realizaron al personal del Departamento Técnico Informático de la Carrera de Ingeniería en Sistemas Computacionales. Con las cuales se conocieron las actividades que se desarrollan dentro y los niveles de seguridad que están implementados.

- ✓ Asignar a un Responsable de la Seguridad Informática en software, que realice y supervise las funciones relacionadas con la seguridad informática de la CISC.
- ✓ Elaborar, Documentar y poner en marcha un manual de políticas y normas de seguridad informática en software en la CISC.
- ✓ Realizar modificaciones de acuerdo a las necesidades existentes al momento de forma transparente al manual de políticas y normas de seguridad informática en software de la CISC.
- ✓ Asignar los recursos necesarios para la gestión de seguridad informática en software, independiente de la unidad de informática.
- ✓ Definir cuáles serían los objetivos de la seguridad informática en software en la CISC.
- ✓ Actualizarse cada vez que sea necesario sobre estándares internacionales en temas de seguridad informática en software.

- ✓ Incluir además del personal del departamento técnico a directivos de la institución en temas de seguridad informática en software.
- ✓ Concienciar a los usuarios, en temas de seguridad informática en software, hacerles sentirse responsables y parte de la institución.
- ✓ Capacitar a los empleados de la institución en temas de seguridad, adoptando un estricto control de las técnicas más comunes de seguridad informática en software.