Universidad de las Ciencias Informáticas

"FACULTAD 8"

Gestión del ambiente de producción del Proyecto CICPC

Trabajo de Diploma para optar por el título de

Ingeniero en Ciencias Informáticas

Autores: David Vázquez Torres.
Banier Reyes Saiz.

Tutor: Ing. Nilet Soto López.

Co-Tutor: Ing. Yohandri Rill Gill.

Ciudad de la Habana, Junio 2008.

"Año 50 de la Revolución"

DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo a la Facultad 8 de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los __ días del mes de_____ del año ____.

David Vázquez Torres.

_____

Firma del autor.

Banier Reyes Saiz

_____

Firma del autor.

Ing. Nilet Soto López.

_____

Firma del tutor.

Lo que sabemos es una gota de agua; lo que ignoramos es el océano.

Isaac Newton.

AGRADECIMIENTOS

A nuestro comandante en Jefe Fidel Castro Ruz, por ser el creador de esta universidad.

A nuestra familia por todo el amor y apoyo que nos han brindado a lo largo de todos estos años.

A nuestros padres el sacrificio, el amor, las enseñanzas, y el apoyo que nos han dado convirtiéndome en el hombre que soy.

A la profesora Lesyanis Pompa Arcia por su incondicional ayuda en la elaboración de este documento.

Al Ing. Yohandri Rill Gil que sin su ayuda no se hubiesen logrados los resultados obtenidos.

Al Ing. Rigoberto Riverón Pérez por su ayuda con las herramientas de Gestión de la Red.

A todo aquel de una manera u otra ayudaron al desarrollo y elaboración de este documento.

DEDICATORIA.

David.

A mi madre que gracias a ella soy lo que soy hoy. A mi padre que siempre supo guiarme y confiar en mí.

En especial a mi Abuela Eva que siempre estuvo al lado mío, siempre te voy a llevar en mi corazón.

Banier.

A mi madre que lo ha dado todo por mí y nunca ha dejado de confiar en su hijo. A mi padre que de siempre lo llevo en el corazón.

RESUMEN

En los últimos años las Tecnologías de la Informatización y las Comunicaciones (TIC) han tenido un gran auge a nivel internacional y en especial en nuestro país. Gracias al incremento de los servicios en el área del Desarrollo de Software en los cuales se inserta la Universidad de las Ciencias Informáticas (UCI), se han efectuado numerosos convenios en el campo del desarrollo de aplicaciones informáticas; donde el Proyecto de Informatización del "Cuerpo de Investigaciones, Científicas, Penales y Criminalísticas" (CICPC) se está llevando a cabo actualmente; en este marco de trabajo, se hace necesaria la creación de un "Entorno Controlado de Desarrollo" para los laboratorios de producción, así como establecer una estrategia para la administración y configuración de los servidores que van a ser usados en el montaje de los servicios necesarios para el desarrollo de los aplicativos. Consecuencia de esto se hace imprescindible la creación e implantación de un Plan de Seguridad Informática que regule el acceso a las computadoras y a los servidores, además de la protección y seguridad a la que debe estar sujeta la información que se maneja. El presente trabajo se propone mejorar los procesos llevados a cabo para la creación de un ambiente de desarrollo adaptable a un equipo multidisciplinario de desarrollo, y la exposición de los resultados obtenidos mediante la implantación de los mismos.

PALABRAS CLAVES: Ambiente, Desarrollo, Entorno, seguridad, configuración, servidores.

ÍNDICE.

TABLA DE CONTENIDO

INTRODUCCIÓN 1
CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA 5
1.1- Introducción. 5
1.2- Desarrollo. 5
1.3- Seguridad Informática. 6
1.3.1- ¿Cómo establecer los requisitos de seguridad? 6
1.3.2- Punto de partida de la seguridad de la información. 7
1.3.3- Factores críticos de éxitos. 7
1.3.4- Plan de seguridad Informática. 9
1.4- Herramientas para la gestión de red. 10
1.4.1- Herramientas de monitoreo de red. 11
1.4.2- Descripción de los programas de monitoreo de red. 12
1.4.3- Resultados obtenidos en el monitoreo. 14
1.5- Entornos Controlados de Desarrollo. 16
1.6- Servidores. 16
1.6.1- Tipos de servidores. 16
1.6.3- Privilegios y Complejidad. 18
1.7- Propuesta de Solución. 19
1.8- Conclusiones. 20
CAPÍTULO 2: PLAN DE SEGURIDAD INFORMÁTICA 21
2.1- Introducción. 21
2.2- Desarrollo. 21
2.2.1- Caracterización del Sistema Informático. 21
2.2.2- Servicios en Explotación. 22
2.2.3- Procesamiento de la información limitada y confidencial. 23
2.2.4- Solución. 23
2.2.4.1- Identificación de los activos informáticos. 23
2.2.4.2- Evaluación de los activos informáticos. 24
2.2.4.3- Identificación de amenazas. 25
2.2.4.4- Estimación de los riesgos sobre los bienes informáticos. 28
2.2.5- Resultados del Análisis de Riesgo. 30
2.3- Medidas. 31
2.3.1- Elaboración del tiempo de máquina. 32
2.3.2- Medidas de Seguridad Técnicas o Lógicas. 33
2.3.2.1- Identificación y autentificación de usuarios. Protección de entrada a las tecnologías de la información. 33
2.3.2.2- Control de uso de los recursos y de la información. 33
2.3.2.3- Medidas que garantizan la integridad de la información. 34

2.3.2.4- Seguridad y uso correcto de los medios. 36
2.3.2.5- Control del uso, traslado y entrada de tecnologías de la información. 36
2.3.3- Contratos a terceros. 37
2.3.3.1- Inicio de la guardia. 38
2.3.3.2- Durante la guardia. 38
2.3.3.3- Final de la guardia. 40
2.3.4- Guardia estudiantil en el turno de noche. 40
2.3.5- Sanciones disciplinarias. 41
2.3.5.1- Disposiciones generales. 41
2.3.5.2- Faltas Leves. 41
2.3.5.3- Faltas Graves. 42
2.3.5.4- Faltas muy Graves. 42
2.4- Conclusiones. 42
CAPÍTULO 3: ESTRATEGIA DE ADMINISTRACIÓN Y CONFIGURACIÓN DEL ENTORNO CONTROLADO DE DESARROLLO 43
3.1- Introducción. 43
3.2- Características del Entorno. 43
3.2.1- Hardware. 43
3.2.2- Organizacionales. 44
3.2.3- Software 45
3.3- Descripción de la base para el ambiente de producción. 51
3.4- Criterios a tener en cuenta para la configuración. 52
3.5- Procedimientos 53
3.5.1- Preparación de las imágenes. 53
3.5.2- Montaje de las imágenes. 55
3.5.3- Mantenimiento del hardware de la computadora. 56
3.5.4- Actualización del hardware de la computadora. 57
3.5.5- Mantenimiento de software. 58
3.5.6- Actualización de software. 59
3.5.7- Actualizar políticas de seguridad. 60
3.5.8- Proceso de auditoría. 60
3.6- Conclusiones. 61
CAPÍTULO 4: ESTRATEGIA DE ADMINISTRACIÓN Y CONFIGURACIÓN DE LOS SERVIDORES 62
4.1- Introducción. 62
4.2- Características de los servidores. 62
4.2.1- Hardware 62
4.2.2- Servicios generales. 64
4.2.3- Servicios específicos 65
4.2.4- Servicios ya implementados que se van a usar: 66

4.2.5- Herramientas para el cumplimiento de los servicios..... 67
4.2.6- Distribución de los servicios. 69
4.2.7- Selección de los sistemas operativos. 70
4.3- Criterios a tener en cuenta para la configuración. 71
4.4- Políticas de respaldo y recuperación. 73
4.4.1- Reglas para el respaldo. 74
4.4.3- Proceso para el respaldo y recuperación de la información. 74
4.4.3.1- ¿Qué es lo importante a respaldar? 74
4.4.3.2- Tipos de respaldo a realizar. 75
4.4.3.3- Cantidad de respaldos a realizar. 76
4.4.3.5- Localización de los respaldos. 76
4.4.3.6- Recuperación ante fallos. 76
4.5- Conclusiones. 76
CAPÍTULO 5: RESULTADOS OBTENIDOS 77
5.1- Introducción. 77
5.2-Beneficios de la creación del Entorno controlado de Desarrollo. 77
5.2.1- Tiempo ahorrado. 78
5.2.2- Datos recogidos con el transcurso del tiempo. 79
5.3- Servidores. 82
5.4- Proceso de auditoría para las computadoras del Proyecto CICPC. 84
5.4.1- GFI LANGuard N.S.S. 84
5.4.2- GFI LANGuard S.E.L.M. 86
5.5- Conclusiones. 87
CONCLUSIONES 88
RECOMENDACIONES 89
REFERENCIA BIBLIOGRÁFICA 90
BIBLIOGRAFÍA 91
GLOSARIO DE TÉRMINOS 94
ANEXOS 95
[Anexo 1]. Instalación y configuración del Jakarta Tomcat en HP-UX 11i v2. 95
[Anexo 2]. Instalación y configuración del SubVersioN. 100
[Anexo 3]. Instalación del Trac con Python 2.5.1 102
[Anexo 4]. Modelo 1: Planificación del Tiempo de Máquina. 109
[Anexo 5]. Modelo 2: Libro de Incidencias. 109
[Anexo 6]: Modelo 3: Libro de Visita. 110
[Anexo 7]. Modelo 4: Solicitud de Mantenimiento. 110
[Anexo 8]. Modelo 5: Registro de soportes magnéticos. 110
[Anexo 9:]. Modelo 6: Registro de entrega/recepción de soportes magnéticos. 111

INTRODUCCIÓN

Uno de los aspectos más importantes del mundo contemporáneo, es el desarrollo creciente de la ciencia y la tecnología, abarcando todas las esferas de la vida del hombre; la informática como parte importante de esta se convierte en uno de los puntales del desarrollo económico del planeta. El mismo desarrollo en si ha condicionado la ausencia de seguridad en las redes informáticas, propiciando la pérdida de información confidencial y la aparición del delito informático. Ello ha motivado el interés, por investigar, cómo implementar Planes de Seguridad Informática para los laboratorios de proyectos que garantice la integridad de la información contenida en estos. En tal sentido el trabajo de diploma está relacionado al tema de la gestión del ambiente de desarrollo en un proyecto.

En el 2006 gracias a los acuerdos de cooperación entre la República Bolivariana de Venezuela y Cuba, la Universidad de las Ciencias Informáticas (UCI) se ha visto involucrada en varios proyectos de informatización, entre ellos se puede mencionar el Proyecto de Modernización del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas de Venezuela *(*a partir de ahora se hará referencia como CICPC*)*, perteneciente al Ministerio del Poder Popular para Relaciones Interiores y Justicia (MPPRIJ); relacionado con el desarrollo e implementación de un nuevo Sistema de Investigación e Información Policial (SIIPOL), tomando como referencia el sistema de Información Policial existente.

Para ello la Facultad 8 creó el Proyecto CICPC, y puso a disposición de un equipo multidisciplinario de estudiantes y profesores, una serie de computadoras para la ejecución del proyecto; las mismas quedaron distribuidas en dos (2) laboratorios de desarrollo, los cuales no cuentan con un ambiente de producción adecuado para el desarrollo de los productos de software; además la seguridad de la red de los laboratorios no es la ideal para un proyecto de esta magnitud, ya que se manejan datos confidenciales y cualquier entrada o acceso a las computadoras no autorizada podría poner en peligro la integridad de los datos. En lo que respecta a los servidores necesarios que también fueron suministrados para el proyecto, también se evidencian algunas debilidades referidas a problemas de configuración de los servicios y acceso a los mismos, lo que imposibilita la ejecución en tiempo de las pruebas al sistema e incluso el avance del trabajo de producción diario; además no hay una política que permita el respaldo diario de la información, siendo esto uno de los riesgos críticos a tener en cuenta en un proyecto.

Por consiguiente el **problema a resolver** consistiría en ¿Cómo crear un ambiente de desarrollo adecuado y adaptado a las necesidades de un equipo de producción con el objetivo de desarrollar las aplicaciones en el Proyecto CICPC?

INTRODUCCIÓN.

Por lo anteriormente expuesto el trabajo de investigación está sustentado en la siguiente **idea a defender**: si se crea e implementa un adecuado Plan de Seguridad Informática y monitoreo para los laboratorios y los servidores del proyecto, se podría garantizar un ambiente de desarrollo adecuado para desarrollar las aplicaciones en el Proyecto CICPC, garantizando a su vez la detección de intrusiones o incumplimiento de las políticas de seguridad establecidas.

El **campo de acción** se considera los laboratorios de producción del Proyecto CICPC; cuyo **objeto de estudio** está dado por la gestión de un ambiente de desarrollo robusto y estable que satisfaga las necesidades de los grupos de trabajo.

Como **objetivo general** se plantea crear e implementar un ambiente de desarrollo seguro, robusto y estable que permita llevar a cabo la producción de los artefactos del software y las pruebas en un ambiente similar al de despliegue en Venezuela. Para dar cumplimiento a este objetivo se generaron las siguientes **tareas de la investigación:**

1. Se realizará una investigación referente a la seguridad informática y sus normativas, específicamente para los laboratorios de proyecto dentro de la universidad.
2. Se estudiará el flujo de trabajo de Gestión de Ambiente del Proceso Unificado de Desarrollo (RUP) y roles relacionados a la gestión de ambiente.
3. Se investigará y se realizará una selección de herramientas de software necesarias para la producción.
4. Se investigará acerca de las configuraciones de los servidores, específicamente de sistemas operativos como Ubuntu 7.04 server, HP-UX 11i v2.y Windows Server 2003.
5. Se estudiarán las principales herramientas de gestión de la configuración y la seguridad que se usan a nivel internacional, nacional, en la universidad y se realizará una comparación para seleccionar cual se ajusta a las necesidades del proyecto.
6. Se realizará una investigación mediante la cual se espera recopilar los principales problemas que hay en la universidad, sobre todo en el área de los laboratorios de proyecto con la seguridad de las computadoras de desarrollo.
7. Se estudiará sobre las políticas de seguridad de la universidad que sirvan de apoyo en la elaboración del plan de seguridad del proyecto.
8. Se investigará a fondo las características del hardware de los servidores del proyecto para seleccionar los servicios que van a ser instalados en cada uno.
9. Se elaborará e implementará la propuesta del Plan de Seguridad Informática para los laboratorios del Proyecto CICPC.

10. Se instalarán y se configurarán los servidores del proyecto.
11. Se pondrán a prueba las herramientas seleccionadas para la gestión de la configuración y la seguridad, para así detectar los principales problemas de seguridad.

Para lograr una correcta organización del documento y dar cumplimiento a los objetivos trazados en la investigación, se propone el desarrollo de los siguientes capítulos:

Capítulo 1: Fundamentación Teórica.

Este capítulo se refiere a los resultados de las investigaciones relacionadas con el tema del trabajo, tanto en el ámbito internacional como nacional, explicando los conceptos esenciales relacionados con la gestión de ambiente y entornos controlados de desarrollo. Se aborda el tema de la seguridad desde el marco nacional particularizando en nuestra universidad, para de esta manera saber ¿Qué se viene haciendo en nuestro país y en la UCI para la protección de los activos informáticos? Por último se hace un análisis de las herramientas para la gestión de la red y se brinda un acercamiento a los servidores y sus distintas funcionalidades.

Capítulo 2: Plan de Seguridad Informática.

En este capítulo se presenta el Plan de Seguridad Informática para el Proyecto CICPC, se detallan las amenazas a las que están expuestos los activos informáticos y se exponen cuales son las principales vulnerabilidades en los posibles ataques de intrusos. Se dan a conocer las medidas elaboradas para la protección de dichos activos informáticos organizadas por secciones y artículos, así como las sanciones disciplinarias a tomar ante cualquier violación de un artículo.

Capítulo 3: Estrategia de administración y configuración del Entorno Controlado de Desarrollo.

En este capítulo se presenta la propuesta de creación y configuración del ambiente de producción para el Proyecto CICPC. Se detallan y caracterizan el conjunto de herramientas que deben ser instaladas y configuradas, además de la serie de pasos o procedimientos a seguir en caso de que se realice una actualización o mantenimiento, ya sea de hardware o software, y las medidas a tomar en caso de que hayan cambios en las políticas de seguridad implantadas para asegurar que se cumpla el Plan de Seguridad Informática.

Capítulo 4: Estrategia de administración y configuración de los servidores.

En este capítulo se exponen las características físicas de los servidores del Proyecto CICPC, así como los servicios con que actualmente cuenta el proyecto. Se realiza y explica el proceso para las copias de seguridad adoptadas en caso de que ocurra una falla del sistema poder recuperar la información perdida.

Capítulo 5: Resultados obtenidos.

En este capítulo se dan a conocer los resultados de la implantación del entorno controlado de desarrollo para el Proyecto CICPC. Además se exponen detalles de los procesos de auditoría y las medidas tomadas en cada caso según los artículos del Plan de Seguridad Informática.

CAPÍTULO 1

FUNDAMENTACIÓN TEÓRICA

1.1- Introducción.

En el presente capítulo se expondrán temas relacionados con la administración de redes, haciendo énfasis en los conceptos generales del Plan de Seguridad Informática, la gestión de la red como alternativa para mantener la confidencialidad de la información que se maneja y una explicación de que es un “Entorno Controlado de Desarrollo”. Lo anterior servirá de apoyo para un mejor análisis de cómo llevar a cabo de forma idónea una administración de sistemas.

1.2- Desarrollo.

Las redes de cómputos de las organizaciones, se vuelven cada vez más complejas y las exigencias de las operaciones es cada vez más demandante. Las redes, cada vez más, soportan aplicaciones y servicios estratégicos de las organizaciones.

Hoy en día las amenazas a la seguridad de información, como Internet, gusanos, ataques de denegación de servicio, virus y otras intrusiones son más sofisticadas, frecuentes y peligrosas que nunca. Además, el espectacular aumento de las vulnerabilidades descubiertas, junto con la velocidad a la que se crean nuevas amenazas hace de este reto aún mayor. La medición y la gestión de la red de riesgo es un reto importante para las empresas de todos los tamaños.

Gracias al creciente avance de la ciencia y la tecnología, que ha traído consigo la generación, transmisión y manipulación de una inmensa cantidad de información surge el tema de la administración de redes, que no es más que el conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Para mantener una red segura y constantemente monitoreada contra los ataques, surge el tema de la seguridad informática.

1.3- Seguridad Informática.

Se entiende como seguridad un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo.

Las normativas NC-ISO-IEC 17799 y NC-ISO-IEC 27001, pertenecientes a los estándares internacionales ISO (Organización Internacional de Normalización, estipulan cómo debe hacerse un correcto Plan de Seguridad Informática, las mismas han sido elaboradas por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información, en el que están representadas las siguientes organizaciones [NC-17799][NC-27001]:

- Ministerio de la Informática y las Comunicaciones.
- SEGURMÁTICA.
- DESOFT.
- Universidad de las Ciencias Informáticas (UCI).
- Universidad de Villa Clara.
- Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMATEL).
- Instituto Superior Politécnico José Antonio Echeverría. (ISPJAE)
- Ministerio de Salud Pública (Centro de Control Estatal de Equipos Médicos).
- Oficina de Seguridad de las Redes Informáticas.
- Oficina Nacional de Normalización.

La definición de seguridad informática según las normativas NC-ISO-IEC 17799 y NC-ISO-IEC 27001, no es más que la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad informática se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados y mejorados cuando sea necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

1.3.1- ¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales:

- La primera fuente procede de la valoración de los riesgos de la organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima su posible impacto.

- La segunda fuente es el conjunto de requisitos legales, estatuarios, normativos y contractuales que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.
- La tercera fuente está formada por los principales, objetivos y requisitos que forman parte del procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

1.3.2- Punto de partida de la seguridad de la información.

Un cierto número de controles pueden ser considerados como un buen punto de partida para implementar la seguridad informática. Estos están basados en requisitos legislativos esenciales o que se consideran práctica habitual de la seguridad de la información. Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden, dependiendo de la legislación aplicable:

- La protección de los datos y la privacidad de la información de carácter personal.
- La protección de los registros de la organización.
- Los derechos de la propiedad intelectual.

Los controles que se consideran práctica habitual para conseguir la seguridad informática, comprenden:

- La documentación de la política de seguridad informática.
- La asignación de responsabilidades de seguridad.
- La concienciación, formación y capacitación en seguridad informática.
- El correcto procesamiento de las aplicaciones.
- La gestión de la vulnerabilidad técnica.
- La gestión de la continuidad del negocio.
- La gestión de incidentes de seguridad informática y mejoramiento.

Estos controles pueden aplicarse a la mayoría de las organizaciones y en la mayoría de los ambientes.

1.3.3- Factores críticos de éxitos.

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implementación de la seguridad informática en una organización:

- Una política de seguridad, objetivos y actividades que reflejen los objetivos del negocio de la organización.
- Un enfoque para implantar la seguridad que sea consistente con la cultura de la organización.

- El apoyo visible y el compromiso de la alta dirección.
- Una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo.
- La comunicación eficaz de la necesidad de la seguridad a todos los directivos y empleados.
- La distribución de directrices sobre la política de seguridad informática de la organización y de normas a todos los empleados y contratistas.
- Proveer recursos para las actividades de gestión de seguridad informática.
- Proveer concientización, formación y educación apropiadas.
- Un proceso efectivo de gestión de incidentes de seguridad de la información.
- Implementación de un sistema de medición utilizado para evaluar el desempeño en la gestión de seguridad informática y las sugerencias de mejoras.

La información es uno de los activos más importantes tanto en el sector privado que público; definir, alcanzar, mantener y mejorar la seguridad informática puede ser esencial para evitar los ataques, amenazas y vulnerabilidades a las cuales está expuesta. Con el creciente desarrollo de la informática y el rápido crecimiento de las redes informáticas han surgido amenazas de seguridad procedentes de una amplia variedad de fuentes, incluyendo fraudes informáticos, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como códigos malignos y ataques de intrusión o de denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Los medios para impedir estas amenazas son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Por todo lo antes expuesto se considera que la realización de un Plan de Seguridad Informática junto con la identificación de los controles que deberían instalarse se hace de esencial importancia en cualquier empresa donde existan computadoras interconectadas entre sí.

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado.
- **Confidencialidad**: La información debe ser solo para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad**: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

Un Plan de Seguridad Informática está regido por las **políticas de seguridad**, que tienen como objetivo principal el de proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos del proyecto y con las regulaciones y leyes pertinentes.

1.3.4- Plan de seguridad Informática.

Un Plan de seguridad Informática, no es más que el conjunto de las medidas de seguridad y protección de la información y de disciplina informática, que comprende medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo o constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías informáticas y de comunicaciones; así como el correcto uso y conservación de las mismas.

El Plan de Seguridad Informática constituye una exigencia de la Resolución No. 6 de 1996 del Ministerio del Interior (MININT) que pone en vigor el Reglamento sobre la Seguridad Informática, en el cual se reflejan las políticas, estructuras de gestión y el sistema de medidas que se determinaron en una institución dada, para lo que se han tenido en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidades realizados en cada objetivo informático del centro y en dependencia de las características de cada área de trabajo.

El Plan de Seguridad Informática está compuesto por un Plan de Contingencia, en el mismo se refleja las medidas que deben tomarse con el fin de garantizar la continuidad de los procesos informáticos ante cualquier desastre o eventualidad que puedan provocar su

interrupción en cada área y las acciones necesarias para contrarrestarlas o enfrentarlas en el menor plazo posible.

1.4- Herramientas para la gestión de red.

Para poder efectuar una administración de redes más segura y eficiente, esta se tiene que auxiliar en varias técnicas que le ayuden a filtrar todos los paquetes que son enviados. Una de estas técnicas es el **monitoreo de red**. Una de las cosas más interesantes en el monitoreo de red es saber qué es lo que entra y que es lo que sale de la computadora, y también brinda una idea de todo lo que pasa en la red, desde que se escriba una dirección de internet y se cargue una página web hasta detectar ataques a los equipos conectados a una red. Esto permite administrar mejor la computadora (o red) e inclusive mejorarla basándose en los resultados que aporta [IntMont].

Para entender que es el monitoreo de la red, primero hay que definir el concepto de monitoreo.

El **monitoreo** no es más que el proceso continuo y sistemático mediante el cual se verifica la eficiencia y la eficacia de un proyecto mediante la identificación de sus logros y debilidades y en consecuencia, se recomienda medidas correctivas para optimizar los resultados esperados del proyecto. Es, por tanto, condición para la rectificación o profundización de la ejecución y para asegurar la retroalimentación entre los objetivos y presupuestos teóricos y las lecciones aprendidas a partir de la práctica. Asimismo, es el responsable de preparar y aportar la información que hace posible sistematizar resultados y procesos y, por tanto, es un insumo básico para la evaluación.

Por tanto el término **monitoreo de la red** describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de fallas vía correo electrónico, beeper u otras alarmas. Es un subconjunto de las funciones implicadas en la administración de la red [MontRed].

Tener un monitoreo en tiempo real es de vital importancia para el administrador de sistema, porque así puede tener una visión de cuáles son los principales problemas o vulnerabilidades que afrontan las computadoras y/o la red que administra. Mediante la técnica de monitorización se recogen la información necesaria para que el administrador pueda en un plazo corto de tiempo resolver cualquier situación que se avecine.

Los aplicativos de monitoreo del estado de la red permiten, entre varias cosas:

1. **Revisar los signos vitales de la red en tiempo real**

   Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red monitorea la red de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio.

2. **Estado de respuesta de fallas.**

   Tal como cuando una conexión no puede ser establecida, está en tiempo muerto, usualmente se produce una acción del sistema de monitoreo, que puede ser un mensaje de alerta a la computadora del administrador de sistema o el envío de un correo electrónico dando detalles de los sucedido.

3. **Alerta de cambios en las políticas de seguridad**

   Cuando el sistema de monitoreo de la red encuentra que en una o más computadoras existe un cambio en las políticas de seguridad, automáticamente envía un mensaje de alerta informando cuales fueron los cambios que se hicieron, reportando así el IP y/o nombre la computadora.

1.4.1- Herramientas de monitoreo de red.

Con el pasar del tiempo las herramientas de monitoreo de red se han incrementado en número, en el pasado la monitorización de la red se hacía a través de empresas que ponían a disposición servidores dedicados a esa tarea, cobrando así altísimos precios por este servicio. Hoy en día existen en el mundo numerosas herramientas que han ayudado a innumerables negocios que cuentan con una red de computadoras. Según una encuesta realizada a usuarios en todo el mundo a finales del año 2007, se hizo una selección de cuáles eran las 8 mejores herramientas de monitoreo que se utilizaban. Estas herramientas con su descripción formal se presentan a continuación:

1. Nessus
2. Paquete GFI LANGuard
3. ISS Internet Scanner
4. Core Impact
5. Sara
6. QualysGuard
7. SAINT
8. Microsoft Baseline Security Analyzer

1.4.2- Descripción de los programas de monitoreo de red.

Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola Nessus puede ser programado para hacer escaneos programados con cron. Nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varias exploraciones para atacarlo. Las pruebas de vulnerabilidad, disponibles en una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes [Nessus].

Paquete GFI LANGuard

GFI LANGuard escáner de seguridad de red, es una galardonada solución que le permite escanear, detectar, evaluar y corregir cualquier vulnerabilidades de seguridad en su red. Como administrador, que a menudo tienen que tratar por separado con los problemas relacionados con cuestiones de vulnerabilidad, administración de parches y de la red de auditoría, a veces utilizando múltiples productos. Sin embargo, con GFI LANGuard NSS, estos tres pilares de la gestión de vulnerabilidades se tratan en un solo paquete. Con una sola consola con amplia funcionalidad de presentación de informes, GFI LANGuard NSS La solución integrada le ayuda a abordar estas cuestiones de manera más rápida y eficaz [GFI LANGuard].

Core Impact

Core Impact es la más completa gama de productos para la evaluación de la organización; su habilidad para detectar, prevenir y responder a las amenazas de seguridad de la información es muy efectiva. Al replicar en condiciones de seguridad del mundo real los ataques contra servidores de red y estaciones de trabajo, sistemas de usuario final, y aplicaciones web, Core Impact le ayuda a encontrar y corregir problemas de seguridad de datos antes de producirse los incidentes [CoreImpact].

ISS Internet Scanner

Internet Scanner minimiza su riesgo mediante la identificación de los agujeros de seguridad o vulnerabilidades en la red para que pueda protegerlos ante un ataque. Internet Scanner pueden identificar más de 1300 tipos de dispositivos de red en su red, incluyendo equipos

de escritorio, servidores, routers / switches, “cortafuegos”, dispositivos de seguridad y la aplicación routers.

Una vez que todos los dispositivos de su red se identifican, Internet Scanner analiza las configuraciones, los niveles de parches, sistemas operativos y aplicaciones instaladas para encontrar vulnerabilidades que podrían ser explotadas por piratas informáticos tratan de obtener acceso no autorizado [InternetScanner].

SARA

La Seguridad del Auditor Asistente de Investigación (SARA) de tercera generación es una herramienta de análisis de la seguridad de la red que presenta las siguientes características:

- Opera bajo Unix, Linux, MAC OS / Windows (a través de coLinux) OS.
- Integra la Base de Datos Nacional de la Vulnerabilidad (NVD).
- Realiza pruebas de inyección de SQL.
- Puede adaptarse a los entornos de muchos cortafuegos.
- Apoyo a distancia libre de exploración y las instalaciones de la API.
- Plug-in para la instalación de aplicaciones de terceros.
- Libre uso de licencia abierta orientada a SATAN
- El usuario de extensión de apoyo.

Una reciente adición a SARA es la capacidad de operar en un 2K Windows y las plataformas Windows XP. SARA se basa en la Cooperativa de Linux para proporcionar el entorno operativo adecuado para operar como Windows proceso. Este producto se denomina coSARA [SARA].

QualysGuard

QualysGuard es un sistema de monitoreo de red que descubre todos los activos a través de la red, recoge detalles de acogida incluyendo el sistema operativo y los servicios abiertos. Administra la red por la categorización de los activos en grupos o unidades de negocio. Asigna un valor empresarial a los grupos de activos sobre la base de su criticidad a la operación de un negocio. Determina un perfil de riesgo de referencia para que pueda centrarse en la eliminación de riesgos de activos sobre la base de la criticidad. Identificar las vulnerabilidades de seguridad de manera regular con una agenda automatizada. Medir el nivel de los riesgos de negocio relacionados a los activos de acuerdo a políticas de seguridad [QualysGuard].

SAINT

SAINT es el Administrador de Seguridad de la Red Integrada. En su modo más simple, se reúne a la mayor cantidad de información acerca de redes y hosts remotos como sea posible mediante el examen de los servicios de red tales como dedo de la mano, NFS, NIS, ftp y tftp, rexd, statd, y otros servicios. La información recogida incluye la presencia de varios servicios de información de la red, así como posibles fallas de seguridad, por lo general en forma de configuración de los servicios de red [SAINT].

Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer es una sencilla herramienta con la que se puede realizar un análisis automático del sistema en busca de posibles vulnerabilidades y fallos de seguridad. El análisis se efectúa automáticamente, sin necesidad de intervención por parte del usuario, ni de conocimientos previos de administración. Sólo se necesita seleccionar el ordenador que se quiere analizar, y requiere de privilegios de administración en dicha computadora [MBSA].

1.4.3- Resultados obtenidos en el monitoreo.

Los resultados de las herramientas de gestión de la red proporcionan información valiosa que brinda soporte a la administración eficiente de la red y otras medidas de seguridad que mejoran la protección contra ataques por internet.

El reporte de monitoreo describe el tipo de vulnerabilidad o riesgo, da un diagnóstico de los temas y problemas asociados, y brinda orientación sobre la forma en que se pueden resolver o parchar las vulnerabilidades aisladas. Los reportes asignarán una clasificación a las vulnerabilidades identificadas durante el proceso de escaneo.

Niveles de vulnerabilidades que reporta el monitoreo.

Nivel 5: Las vulnerabilidades Nivel 5 dan a los intrusos acceso remoto al sistema con capacidad root o de administrador. En este nivel de vulnerabilidad el intruso puede comprometer la seguridad del host completo. El Nivel 5 incluye vulnerabilidades que dan a los intrusos capacidades remotas completas de lectura y escritura del sistema, ejecución remota de comandos como usuario root o administrativo.

Nivel 4: Las vulnerabilidades Nivel 4 dan a los intrusos capacidades de usuario remoto, pero no de administrador o usuario root. Las vulnerabilidades Nivel 4 dan a los intrusos acceso parcial a los archivos y sistemas (por ejemplo, acceso total de lectura sin acceso de escritura completo). Las vulnerabilidades que exponen la información confidencial de alta sensibilidad también se consideran Nivel 4.

Nivel 3: Las vulnerabilidades Nivel 3 dan a los intrusos acceso a información específica guardada en el host incluyendo las programaciones de seguridad. Este nivel de vulnerabilidad podría traer como resultado un uso indebido potencial del host. Los ejemplos de vulnerabilidades Nivel 3 incluyen divulgación parcial del contenido de los archivos, acceso a ciertos archivos del host, navegación de directorios, divulgación de reglas de filtrado y mecanismos de seguridad, susceptibilidad a ataques de negación de servicio y uso no autorizado de servicios como reenvío de correo.

Nivel 2: Las vulnerabilidades Nivel 2 exponen algunos tipos de información confidencial del host, tales como versiones precisas de los servicios. Si tiene esta información el delincuente puede investigar la forma de lanzar ataques contra un host.

Nivel 1: Las vulnerabilidades Nivel 1 exponen información, tales como puertos abiertos.

Estos niveles de vulnerabilidades son de gran importancia porque da una medida de cuan vulnerable es la red que se administra y cuáles son los posibles objetivos de un intruso a la hora de atacar [SegDatos].

La tabla 1 muestra una comparación entre las diferentes herramientas de monitoreo, para ello se tienen en cuenta los siguientes aspectos:

- Monitoreo en tiempo real.
- Sistema operativo que soporta.
- Plataforma.
- Interfaz.

Tabla 1: Comparación de las herramientas de monitoreo de red.

Programas de monitoreo de red.	T. Real.	S.O	Propietario.	Interfaz.
Nessus	SI	W, L, X, U	SI	Gráfica
Paquete GFI LANGuard	SI	W	SI	Gráfica
Core Impact	SI	W	SI	Gráfica
ISS Internet Scanner	SI	W	SI	Gráfica
Sara	NO	W, L, X, U	NO	Comando
QualysGuard	SI	W, L, X, U	SI	Gráfica
SAINT	NO	L, X, U	SI	Gráfica
MBSA	NO	W	NO	Gráfica

Leyenda: L: Linux **W**: Windows **U:** Unix **X:** Mac OS

1.5- Entornos Controlados de Desarrollo.

Un Entorno Controlado de Desarrollo no es más que la instalación y configuración de un conjunto de herramientas que dan soporte a la creación de un sistema o software. Los Entornos Controlados de Desarrollo pueden ser pequeños o tan grandes como se requiera (en dependencia de las funcionalidades que se van a desarrollar), siempre y cuando se encierren dentro de él todos los recursos necesarios para la puesta en marcha de los aplicativos. Dentro del mismo se incluye el hardware, el cual proporciona la plataforma con las herramientas requeridas.

1.6- Servidores.

Internet es una gigantesca red, que incluye sub-redes de ordenadores interconectados, pero desde un punto de vista funcional las tareas están generalmente agrupadas, de forma que desde esta perspectiva (de su funcionalidad), podemos establecer tres grandes grupos: Servidores, Clientes y Correos o enrutadores.

Un servidor en informática o computación es una computadora en el que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes. Un servidor no es necesariamente una máquina de última generación grande y monstruosa, no es necesariamente un superordenador; un servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente. Todo esto depende del uso que se le dé.

Los servidores por excelencias son las computadoras destinadas únicamente a proveer los servicios de otros programas, o lo mismo, una computadora cuyo propósito es proveer datos de modo que otras computadoras puedan utilizar esos datos.

1.6.1- Tipos de servidores.

Existen disimiles tipos de servidores en el mundo, los hay desde funciones pequeñas hasta los que prestan grandes servicios a grandes cantidades de usuarios. A continuación se presentarán algunos ejemplos de servidores:

Servidores de Aplicaciones.

Designados a veces como un tipo de “middleware” (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

Servidores de Chat.

Los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

Servidores FTP.

Uno de los servicios más antiguos de Internet, File Transfer Protocol permite mover uno o más archivos entre las computadoras de la red.

Servidores Groupware.

Un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

Servidores de Correo.

Casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

Servidores Proxy.

Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

Servidores Telnet.

Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

Servidores de Web.

Básicamente, un servidor web sirve de contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

Servidores de archivos.

Una empresa en la que se administre un gran número de documentos puede utilizar un servidor de archivos para un almacenamiento centralizado que permite crear una especie de biblioteca de documentos. Cuando un usuario necesita un archivo, lo busca en el servidor de archivos, trabaja con él localmente en su escritorio y después lo devuelve.

Servidores DNS.

Se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando este está bien configurado.

Servidores de Base de datos.

Un servidor de base de datos es un software que proporciona servicios de bases de datos a otras computadoras clientes o a otros servidores, tal como se define en el modelo cliente-servidor.

1.6.2- Paradigma Cliente-Servidor.

Como se explica anteriormente, los servidores son computadoras que actúan como "almacenes" de información. Esta información es solicitada por los ordenadores-cliente, y el servidor responde a tales peticiones devolviendo los datos solicitados. Este paradigma de funcionamiento Cliente-Servidor es utilizado constantemente en la informática distribuida (donde existen muchas computadoras interconectadas).

El paradigma Cliente-Servidor no es más que la división de las aplicaciones comunicantes en dos categorías, dependiendo de si la aplicación se queda en espera de conexiones (servidor) o las inicia (cliente).

El paradigma cliente-servidor no solo se utiliza en referencia a las computadoras físicas, también a los programas que las hacen funcionar según su utilidad. Por ejemplo, son frecuentes expresiones tales como "cliente de correo" o "servidor de noticias" en referencia a programas. La primera se refiere al que se utiliza normalmente para interrogar al buzón e-mail, descargar el correo y manipularlo (leerlo, imprimirlo, eliminarlo). El segundo se refiere a un programa o sistema de ellos, que en un servidor (computadora) realiza el trabajo de guardar los mensajes de noticias, y atender las peticiones de los "clientes".

1.6.3- Privilegios y Complejidad.

Debido a que los servidores a menudo tienen la necesidad de acceder a datos, funciones, o puertos que el sistema operativo protege, el software servidor suele precisar de privilegios del sistema especiales para poder realizar la tarea para la cual ha sido creada. Como consecuencia de esto se tiene mucho cuidado para evitar que los privilegios concedidos al servidor sean aprovechados por los clientes para obtener permisos especiales. Por ejemplo, un servidor de ficheros que se ejecuta como un programa privilegiado debe contener código para verificar si un cliente dado tiene permisos para acceder a un fichero en concreto. El servidor no puede relegar esta función sobre el sistema operativo, ya que su estado privilegiado le sitúa, en ciertos aspectos concretos, por encima del sistema.

Los programas servidores deben contener código que maneje situaciones de:

- **Autenticación**: Verificar la identidad del cliente.
- **Autorización**: Determinar si un cliente dado posee permisos para acceder al servicio que suministra.
- **Seguridad de datos**: Garantizar que la información no es revelada, de manera no intencionada, a clientes sin autorización.
- **Privacidad**: Preservar la información de un usuario de accesos no autorizados.
- **Protección**: Garantizar que las aplicaciones de red no puedan abusar de los recursos del sistema.

Los servidores que realizan un intensivo uso de la potencia del procesador o que manejan grandes volúmenes de información operan más eficientemente si manejan las solicitudes de servicio concurrentemente. La combinación de privilegios especiales y ejecución concurrente, por norma general, hace que los servidores sean más difíciles de diseñar e implementar que los clientes.

1.7- Propuesta de Solución.

La propuesta de solución para dar respuesta al problema a resolver, consiste en diseñar e implantar un ambiente de desarrollo adecuado y adaptado a las necesidades de los equipos de producción, con el objetivo de desarrollar las aplicaciones del Proyecto CICPC; dicho ambiente involucrará en su diseño la plataforma tecnológica (Hardware y Software) y los procedimientos y reglamentaciones necesarias. Por consiguiente se elaborará un Plan de Seguridad Informática para los laboratorios y servidores del proyecto adaptado a las características particulares del proyecto, para asegurar que se cumpla dicho Plan se implementará una herramienta para la gestión de la configuración y seguridad, además de la selección de los servidores que se van a usar e implementar.

Para el desarrollo del Plan de Seguridad Informática del Proyecto CICPC se tomarán como guías las normativas NC-ISO-IEC 17799 y NC-ISO-IEC 27001.

Después de Analizar la tabla comparativa de las herramientas de monitoreo de la red, se llega a la conclusión que la mejor herramienta para la gestión de la red del Proyecto CICPC es el: **Paquete GFI LANGuard**, ya que fue desarrollada para generar reportes exactos del estado de la red y las computadoras que la integran, además tiene las siguientes ventajas:

- Comprueba automáticamente la contraseña de la política para todas las máquinas en la red.
- Controles para los programas que corren automáticamente (posibles troyanos).

- Descubre si el sistema operativo publica demasiada información.
- NetBIOS proporciona el nombre de host, nombre de usuario actualmente conectado y la dirección MAC.
- Proporciona una lista de acciones, a los usuarios (información detallada), servicios, sesiones, TOD remoto (hora del día) y el registro de información de ordenador remoto (Windows).
- Dispositivo de detección de SNMP, SNMP Walk para inspeccionar dispositivos de red como routers, impresoras de red y más.
- Identifica todos los servicios Windows instalados.

1.8- Conclusiones.

En este capítulo se trataron temas referentes a las normativas para la creación de un Plan de Seguridad Informática que cumpla con todos los requisitos que lleva el mismo, se resumió lo investigado sobre las herramientas de gestión de la red para llevar un monitoreo en tiempo real que ayude a la detección de intrusos en la red de los laboratorios, así como la selección de los servidores que van a ser usados y configurados para el montaje de los distintos servicios con que va a contar el Proyecto CICPC.

CAPÍTULO 2

PLAN DE SEGURIDAD INFORMÁTICA

2.1- Introducción.

Dada la necesidad de garantizar la seguridad y protección de la información que se procesa, se intercambia, se reproduce y se conserva mediante el uso de las tecnologías informáticas y de comunicaciones, y con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, se hace imprescindible la puesta en vigor de un Plan de Seguridad Informática, que regule la disciplina informática a tener en cuenta por todos los integrantes del Proyecto CICPC; en el presente capítulo se presenta la propuesta del mismo.

2.2- Desarrollo.

Para la confección de este Plan de Seguridad Informática y para el estricto cumplimiento de todo lo contenido dentro de él, son objeto de análisis los bienes informáticos y de comunicación que se encuentran dentro de los dominios del Proyecto CICPC. Dicho proyecto se encuentra en La Universidad de las Ciencias Informáticas y cuenta con 2 laboratorios de producción.

2.2.1- Caracterización del Sistema Informático.

- Los bienes informáticos a proteger son cinco (5) servidores, sesenta y dos (62) computadoras, sesenta y seis (66) backups, catorce (14) laptops, equipamiento de la red, un (1) scanner, una (1) impresora, un (1) teléfono, siendo todos ellos de vital importancia para el proyecto.
- El proyecto está organizado en 2 áreas de trabajo fundamentales, laboratorio de producción 207, laboratorio de producción 208 y se incluye el área de la Infraestructura Productiva (a partir de ahora se hará referencia a IP); que nos brinda servicios de hospedaje de un servidor.
- En el laboratorio de producción 207 se encuentran 4 de los 5 servidores:
    - Servidor 1 opera bajo el sistema operativo Windows Server 2003 Enterprise Edition, en él se encuentran los servicios: Integración Continua, Modelado de Base de Datos y Sistema de publicación de aplicaciones Java.

  - Servidor 2 opera bajo el sistema operativo Windows Server 2003 Enterprise Edition, en él se encuentra las herramientas para la gestión de la configuración y seguridad.
  - Servidor 3 opera bajo el sistema operativo GNU/Linux, distribución UBUNTU 7.04, en él se encuentran los servicios: Sistema de control de versiones, Sistema para la gestión de proyectos, Sistema de compartimiento de archivos, Sistema de publicación de aplicaciones PHP, Gestor de base de datos para el Portal Web.
  - Servidor 4 opera bajo el sistema operativo GNU/Linux, distribución DEBIAN 3.1, en él se encuentra el servicio: Gestor de base de datos para el Portal Web.

- En la IP se encuentra el Servidor Integrity, el cual está operando bajo un Sistema Operativo Unix, distribución HP-UX 11i v2; en él se encuentran los servicios: Gestor de base de datos para la Aplicación Web SIIPOL y un Sistema de publicación de aplicaciones Java.
- Cada área tiene un Switch Capa 2 de 10/100 Mbps.
- Los dos laboratorios de producción tienen cada uno un Hub de 6 puertos.
- Las tres aéreas de trabajo cuentan con Backups de respaldo, sistema de alarma contra incendio y están climatizados.
- Los laboratorios de producción cuentan con un grupo de equipos para el desarrollo informático con Sistema Operativo Windows XP Professional, Service Pack 2.

2.2.2- Servicios en Explotación.

La mayoría de los servicios que se encuentran en explotación por los desarrolladores del proyecto fueron a propuesta del cliente o se seleccionaron por la experiencia que tenían los desarrolladores sobre los mismos, estos son:

- Control de versiones.
- Gestión y seguimiento de proyectos.
- Compartimiento de archivos.
- Sistema de integración continua.
- Sistema de modelación de base de datos.
- Publicación de aplicaciones JAVA.
- Gestión de la configuración y la seguridad.

- Publicación de aplicaciones PHP.
- Gestor de base de datos para el Portal Web.
- Gestor de base de datos para la aplicación CICPC.
- Sistema para la gestión de los requerimientos del software.

2.2.3- Procesamiento de la información limitada y confidencial.

En el Proyecto CICPC toda la información es limitada y confidencial, por lo que todas las computadoras deben tener acceso limitado y los usuarios que se conecten deben hacerlo por la cuenta del dominio UCI.CU; la información confidencial se guarda en los servidores del proyecto, a los cuales solo puede tener acceso el personal autorizado.

2.2.4- Solución.

Sobre la base de lo anterior, es necesario actualizar sistemáticamente el análisis de riesgos, utilizando como punto de partida el último realizado y los controles ya implementados, lo que posibilitará que el tiempo y los medios necesarios para su realización sean menores. La siguiente tabla dará inicio a una serie de pasos para cumplir la realización del Análisis y Riesgo.

2.2.4.1- Identificación de los activos informáticos.

Tabla 2: Identificación de activos informáticos.

No	Descripción	Tipo	No. Serie	Ubicación
1	Servidor Integrity	HW		IP
2	Aplicación Web Jakarta Tomcat.	SW		IP
3	Base de Datos Oracle 10g Release 2.	SW		IP
4	Sistema Operativo Unix, distribución HP-UX 11i v2	SW		IP
5	Servidor 1	HW		Laboratorio 207
6	Servidor 2	HW		Laboratorio 207
7	Servidor 3	HW		Laboratorio 207
8	Servidor 4	HW		Laboratorio 207
9	31 computadoras Pentium 4	HW		Laboratorio 207
10	1 Switch Capa 2 de 10/100 Mbps	HW		Laboratorio 207
11	1 Hub de 6 puertos	HW		Laboratorio 207
12	1 Impresora	HW		Laboratorio 207
13	Sistemas operativos Windows XP Professional , Windows Server 2003 Enterprise Edition, GNU-	SW		Laboratorio 207

	Linux, distribución UBUNTU 7.04, GNU-Linux, distribución DEBIAN 3.1			
14	Portal Web.	SW		Laboratorio 207
15	SubVersioN	SW		Laboratorio 207
16	Trac	SW		Laboratorio 207
17	CruiseControl	SW		Laboratorio 207
18	Erwin Studio	SW		Laboratorio 207
19	Paquete GFI LANGuard	SW		Laboratorio 207
20	ProFTPd	SW		Laboratorio 207
21	MySQL Server	SW		Laboratorio 207
22	Requisite Pro.	SW		Laboratorio 207
23	Base de Datos Oracle 10g Release 2	SW		Laboratorio 207
24	3 Laptops Toshiba Satellite	HW		Laboratorio 207
25	1 Laptops Haier	HW		Laboratorio 207
26	31 computadoras Pentium 4	HW		Laboratorio 208
27	1 Switch capa 2 de 10/100 Mbps	HW		Laboratorio 208
28	1 Hub de 6 puertos	HW		Laboratorio 208
29	1 Escaner	HW		Laboratorio 208
30	1 Teléfono	HW		Laboratorio 208
31	Sistema Operativo Windows XP Professional	SW		Laboratorio 208
32	6 Laptops Haier	HW		Laboratorio 208
33	4 Laptops Hewlett Packard	HW		Laboratorio 208

Una vez identificados los bienes informáticos que necesitan ser protegidos es necesario determinar su importancia dentro del sistema informático y clasificarlos según la misma.

2.2.4.2- Evaluación de los activos informáticos.

Tabla 3: Evaluación de activos informáticos.

No.	Dominio	Función	Costo	Imagen	Confid.	Integ.	Disp.	Valor(ω_i)
1	D1	9	9	9	9	9	9	9
2	D1	9	8	9	9	9	9	8.83
3	D1	9	8	9	9	9	9	8.83
4	D1	9	9	9	9	9	9	9
5	D2	8	8	9	9	9	9	8.66
6	D2	7.50	8	7	9	9	8	8.08
7	D2	9	8	9	9	9	9	8.83
8	D2	9	8	9	9	9	9	8.83
9	D2	8	8	7	8	7.50	7	7.58
10	D2	9	9	9	9	9	9	9

11	D2	9	7	9	9	9	9	8.33
12	D2	7	8	6	2	8	8	6.5
13	D2	9	8	9	8	8	8	8.33
14	D2	9	7	9	9	9	9	8.33
15	D2	9	7	9	9	9	9	8.33
16	D2	9	7	9	9	9	9	8.33
17	D2	8	7	7.50	8	8	8	7.75
18	D2	8	7	8	8	8	9	8
19	D2	9	8	7	8	8	8	8
20	D2	7.50	7	6.50	7.50	7	7.50	7.16
21	D2	8	7	8	8	8	8	7.83
22	D2	8	7	8	8	8	8	7.83
23	D2	9	9	9	9	9	9	9
24	D2	8	8	8	3	8	7	7
25	D2	8	8	8	3	8	7	7
26	D3	8	8	7	8	7.50	7	7.58
27	D3	9	9	9	9	9	9	9
28	D3	9	7	9	9	9	9	8.66
29	D3	7	8	6	2	8	8	6.5
30	D3	3	4	2	2	5	4	3.33
31	D3	9	8	9	8	8	8	8.33
32	D3	8	8	8	3	8	7	7
33	D3	8	8	8	3	8	7	7

Leyenda: D1: Infraestructura Productiva, **D2**: Laboratorio de Producción 207, **D3**: Laboratorio de Producción 208.

La determinación de la importancia de los bienes informáticos puede ser realizada de forma descriptiva (por ejemplo, valor alto, medio, bajo) o de forma numérica asignando valores entre cero y diez (0 si no tiene importancia y 10 sí es máxima). La forma numérica tiene la ventaja de que permite estimar el nivel de riesgo con mayor rigor, así como la valoración por áreas o grupos de elementos más fácilmente.

Relación entre los métodos descriptivos y numéricos:

- **0 – 3.5:** Importancia baja
- **3.6 – 5.9:** Importancia media
- **6.0 – 7.9:** Importancia alta
- **8.0 – 10:** Importancia muy alta

2.2.4.3- Identificación de amenazas.

La Tabla 4 permite la realización de un análisis cruzado a partir de la identificación de las amenazas que pueden actuar sobre el sistema informático y su incidencia sobre cada uno de los bienes informáticos que componen el mismo. En cada una de las filas de esta tabla se relacionan las amenazas, numerándolas consecutivamente para su posterior identificación.

Tabla 4: Amenazas contra activos informáticos.

Nº	Amenazas	Activos (Generales)																						
		1	2	3*	4	5*	9*	10*	11*	12	13*	14	15	16	17	18	19	20	21	22	24	25*	29	30	33
1	Acceso no autorizado.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2	Ataques Internos.	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x			x
3	Ataques externos.	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x			x
4	Virus informáticos.	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x			x
5	Modificación de la información.	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x			x
6	Destrucción de información.	x	x	x	x	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x			x
7	Divulgación de información.	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x	x		x
8	Eludir los mecanismos de autenticación o de control de acceso		x	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x
9	Error de programación		x	x				x		x		x	x	x	x	x	x	x	x	x					
10	Fallos de aplicaciones	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x	x					
11	Bugs de S.O y componentes de Windows					x	x				x				x						x	x			x
12	Fallo de energía eléctrica.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x
13	Fallo de hardware.	x			x	x	x	x	x	x											x	x	x	x	x

14	Error de operación.		x	x								x	x	x	x	x	x	x	x	x				
15	Falta de calificación.		x	x	x				x	x														
16	Hurto de activos y/o recursos.	x					x	x	x	x											x	x	x	x	x
17	Inundaciones	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
18	Terremotos	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
19	Incendios	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

*El indicativo * significa que ese activo se va a repetir más de una vez, por tanto, se pone * sobre el número y se especifica en la tabla siguiente los activos que faltan.*

1 Base de Datos Oracle 10g Release 2.	23
Servidor.	6,7,8
30 computadoras Pentium 4.	26
1 Switch Capa 2 de 10/100 Mbps	27
1 Hub de 6 puertos.	28
Sistema Operativo Windows XP	31
1 Laptops Haier.	32

2.2.4.4- Estimación de los riesgos sobre los bienes informáticos.

A partir de las amenazas identificadas en la Tabla 4 se cuantifica el riesgo de que cada una de ellas se materialice sobre cada uno de los bienes informáticos, con ayuda de la Tabla 5.

Tabla 5: Estimación de Riesgos sobre los Activos Informáticos.

No	Dom.	Riesgos																			R_i	ω_i	$R_i * \omega_i$
		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19			
1	D1	0.1	0.1	0.4	0.4	0.2	0.1	0.1			0.2		0.5	0.1			0.1	0.1	0.1	0.1	0.19	9	1.71
2	D1	0.1	0.1	0.4	0.4	0.3	0.2	0.2	0.2	0.3	0.2		0.5		0.3	0.2		0.1	0.1	0.1	0.19	8.83	1.72
3	D1	0.1	0.1	0.4	0.4	0.3	0.2	0.2	0.2	0.3	0.2		0.5		0.3	0.2		0.1	0.1	0.1	0.19	8.83	1.72
4	D1	0.1	0.1	0.2	0.3	0.1	0.1	0.1	0.1		0.1		0.5	0.2		0.2		0.1	0.1	0.1	0.12	9	1.15
5	D2	0.2	0.1	0.3	0.4	0.2	0.1	0.2			0.2	0.5	0.7	0.4				0.1	0.1	0.1	0.18	8.66	1.64
6	D2	0.2	0.1	0.3	0.4	0.2	0.1	0.2			0.2	0.5	0.7	0.4				0.1	0.1	0.1	0.18	8.08	0.45
7	D2	0.2	0.1	0.3	0.4	0.2	0.1	0.2			0.2	0.5	0.7	0.4				0.1	0.1	0.1	0.18	8.83	1.67
8	D2	0.2	0.1	0.3	0.4	0.2	0.1	0.2			0.2	0.5	0.7	0.4				0.1	0.1	0.1	0.18	8.83	1.67
9	D2	0.5	0.4	0.2	0.6	0.4	0.4	0.4			0.2	0.5	0.7	0.5			0.1	0.1	0.1	0.1	0.27	7.58	2.07
10	D2	0.1	0.1	0.2	0.1				0.1	0.1			0.7	0.1			0.1		0.1	0.1	0.09	9	0.85
11	D2	0.1	0.1	0.2	0.1				0.1	0.1			0.7	0.1			0.1	0.1	0.1	0.1	0.1	8.33	0.83
12	D2	0.1					0.1		0.1				0.7				0.2	0.1	0.1	0.1	0.08	6.5	0.51
13	D2	0.2	0.4	0.3	0.5	0.1	0.1	0.1	0.2		0.1	0.3	0.7					0.1	0.1	0.1	0.17	8.33	1.44

14	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.17	8.33	1.44
15	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.17	8.33	1.44
16	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.17	8.33	1.44
17	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2	0.1	0.7		0.2			0.1	0.1	0.1	0.17	7.75	1.35
18	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2	0.1	0.7		0.2			0.1	0.1	0.1	0.17	8	1.36
19	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2	0.1	0.7		0.2			0.1	0.1	0.1	0.17	8	1.36
20	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.18	7.16	1.28
21	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.18	7.83	1.4
22	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.18	7.83	1.4
23	D2	0.2	0.1	0.3	0.2	0.2	0.1	0.4	0.2	0.3	0.2		0.7		0.2			0.1	0.1	0.1	0.18	9	1.62
24	D2	0.1	0.1	0.1	0.5	0.7	0.7	0.7	0.2			0.2	0.7	0.2			0.2	0.1	0.1	0.1	0.24	7	1.73
25	D2	0.1	0.1	0.1	0.5	0.7	0.7	0.7	0.2			0.2	0.7	0.2			0.2	0.1	0.1	0.1	0.24	7	1.73
26	D3	0.5	0.4	0.2	0.6	0.4	0.4	0.4			0.2	0.5	0.7	0.5			0.1	0.1	0.1	0.1	0.27	7.58	2.07
27	D3	0.1	0.1	0.2	0.1				0.1	0.1			0.7	0.1			0.1		0.1	0.1	0.09	9	0.85
28	D3	0.1	0.1	0.2	0.1				0.1	0.1			0.7	0.1			0.1		0.1	0.1	0.09	8.66	0.77
29	D3	0.1						0.2	0.2				0.7	0.1			0.1	0.1	0.1	0.1	0.08	6.5	0.58
30	D3	0.7											0.7	0.4			0.1	0.1	0.1	0.1	0.11	3.33	0.36
31	D3	0.2	0.4	0.3	0.5	0.1	0.1	0.1	0.2		0.1	0.3	0.7					0.1	0.1	0.1	0.17	8.33	1.44

32	D3	0.1	0.1	0.1	0.5	0.7	0.7	0.7	0.2			0.2	0.7	0.2			0.2	0.1	0.1	0.1	0.24	7	1.73
33	D3	0.1	0.1	0.1	0.5	0.7	0.7	0.7	0.2			0.2	0.7	0.2			0.2	0.1	0.1	0.1	0.24	7	1.73

El Peso Relativo del Riesgo sobre cada activo informático se determina mediante la multiplicación del riesgo estimado (R_i) por la importancia relativa del activo (W_i/W_t). La suma de los Pesos Relativos de Riesgos sobre todos los bienes informáticos caracteriza el Peso Total del Riesgo del Sistema (R_t). De modo tal que:

Cálculo para el riesgo relativo de cada dominio.

$$\omega_R(D_i) = \frac{\sum_{i=1}^{n} R_i \times \omega_i}{\sum_{i=1}^{n} \omega_i}$$

Los resultados obtenidos de los cálculos de riesgos para cada dominio y en general es:

Cálculo para el riesgo relativo de todos los dominios.

$$\omega_R = \frac{\sum_{i=1}^{n} R_i \times \omega_i}{\sum_{i=1}^{n} \omega_i}$$

D1 = 0.17
D2 = 0.14
D3 = 0.16
Dt = 0.16

2.2.5- Resultados del Análisis de Riesgo.

Apoyándose en la caracterización y según el estudio realizado, el equipamiento será protegido contra las siguientes contingencias:

- Acceso no autorizado.
- Ataques internos.
- Ataques externos.
- Virus informáticos.
- Modificación de la información.
- Destrucción de la información.
- Divulgación de la información.
- Eludir los mecanismos de autenticación o de control de acceso.
- Error de programación.
- Fallos de aplicaciones.
- Bugs de Sistema Operativo y componentes de Windows.
- Fallo de energía eléctrica.
- Fallo de hardware.
- Error de operación.
- Falta de calificación.
- Hurto de activos y/o recursos.

- Inundaciones.
- Terremotos.
- Incendios.

Una vez realizados los cálculos de riesgos por dominios y en general se llega a la conclusión de que el Laboratorio de Producción 207 es el menos propenso a riesgo de todos los dominios, el más riesgoso es la Infraestructura Productiva, ya que la seguridad de ese local no es manejada directamente por el personal del proyecto y en sentido general, el Proyecto CICPC tiene una baja probabilidad en cuanto a riesgos.

Los activos más importantes para el proyecto son los servidores y los servicios que los mismos brindan, ya que tienen un impacto significativo sobre el Proyecto CICPC en caso de la salida de servicio de alguno de ellos.

2.3- Medidas.

Lo reglamentado en este documento es de estricto cumplimiento, estando sujeto a medidas disciplinarias, cualquier persona que incurra en una falta en dependencia de la gravedad de la misma.

Las computadoras que pertenezcan a los laboratorios del Proyecto CICPC son para uso de todos los estudiantes y profesores que pertenezcan por plantilla al proyecto, y se regulara su utilización mediante el establecimiento de Tiempos de Máquina. Todas las computadoras que pertenezcan al laboratorio deben encontrarse registradas en el dominio UCI, pues así se contempla en el reglamento de nuestra Universidad. El laboratorio debe estar abierto veinte y dos (22) horas del día, los siete (7) días de la semana.

Los estudiantes y profesores que no sean plantilla del Proyecto CICPC solo pueden acceder a los laboratorios de la institución con la autorización del Jefe del proyecto.

Las computadoras y medios informáticos con los que cuenta el Proyecto CICPC solo deben de ser abiertos por el personal de Copextel autorizado, por el Jefe del Proyecto o la Dirección de La Universidad. Dicha operación debe quedar registrada en el Libro de Incidencias (**Ver Anexo 5**).

En caso de detectarse una violación de las puertas o ventanas de los locales del proyecto, o componente informático, se comunicará de inmediato al Jefe de Proyecto, al Jefe de Seguridad y al Equipo de Técnicos de guardia, los que se ocuparán de mantener el local de forma impecable hasta la llegada del personal de la Policía Nacional Revolucionaria (PNR).

2.3.1- Elaboración del tiempo de máquina.

Los tiempos de máquina se medirán en horas de trabajo según tres (3) turnos de cuatro (4) horas cada uno:

- 1er Turno 8:00 AM – 12:00 PM (Mañana)
- 2do Turno 2:00 PM – 6:00 PM (Tarde)
- 3er Turno 8:00 PM – 12:00 AM (Noche)

Artículo 1: Los tiempos de máquina se planificarán de lunes a viernes en tres (3) turnos, y el sábado dos (2) turnos de trabajo. El tiempo fuera de estos horarios es libre para que los estudiantes del proyecto lo empleen para actividades de interés docente.

Artículo 2: La planificadora del proyecto será la responsable directa de asignar los tiempos de máquina según una planificación que debe revisarse semanalmente.

Artículo 3: Se designarán las personas dentro del proyecto que pueden solicitar el tiempo de máquina a la planificadora del proyecto, teniendo en cuenta que esta solicitud deberá llegar una semana antes, con fecha tope del viernes de la semana anterior al plan.

Artículo 4: La solicitud de tiempo de máquina debe ser regida por un formato diseñado al efecto (**Ver Anexo 4**).

Artículo 5: La planificadora puede reservarse el derecho de negar el tiempo de máquina, con la correspondiente notificación, en caso de que los turnos y la cantidad de computadoras no alcancen para cubrir todas las solicitudes.

Artículo 6: El sábado de cada semana debe publicarse para toda la plantilla del proyecto la planificación de los tiempos de máquina y notificarse aquellas solicitudes que no pudieron ser planificadas, con su correspondiente causa.

Artículo 7: La planificadora debe registrar el cumplimiento o no cumplimiento de los tiempos de máquina, pudiendo esto ser utilizado como criterio para priorizar o denegar solicitudes de tiempos de máquina.

Artículo 8: El usuario al que se le ha planificado el tiempo de máquina tiene derecho al mismo hasta pasada la primera media hora, luego dicha computadora puede ser ocupada por cualquier otro miembro del proyecto que la necesite para trabajar, con la seguridad de que no será interrumpido por el usuario planificado anteriormente.

Artículo 9: Cuando el usuario por problemas justificados sepa que no va a poder llegar temprano a su tiempo de máquina, puede notificarlo a su jefe inmediato para que este le garantice que pasada la media hora normada, aún pueda ocupar su puesto de trabajo.

Artículo 10: Se prohíbe la administración en la computadora donde no tenga asignado tiempo de máquina.

2.3.2- Medidas de Seguridad Técnicas o Lógicas.

2.3.2.1- Identificación y autentificación de usuarios. Protección de entrada a las tecnologías de la información.

Artículo 11: Se considera activos informáticos o tecnología de la información a todas las computadoras, tanto de desarrollo como servidores con las que cuenta el proyecto CICPC.

Artículo 12: Se consideran usuarios del Proyecto CICPC a todos los estudiantes, profesores o trabajadores externos de la Universidad que estén en la plantilla del proyecto.

Artículo 13: Todas las computadoras que se considere activo informático del Proyecto CICPC deberán estar integradas al dominio UCI.CU.

Artículo 14: Se impone de forma obligatoria utilizar los mecanismos de identificación (usuario y contraseña del dominio UCI.CU) para acceder a cualquier medio informático del proyecto.

Artículo 15: Es responsabilidad del Jefe de Seguridad del Proyecto CICPC establecer e implementar contraseñas seguras al BIOS de cada computadora, así como cuentas locales de acceso, siendo imprescindible en los servidores, a los cuales solo se accederá de forma remota, aunque para situaciones excepcionales, se podrá tener contacto físico con el servidor.

Artículo 16: La configuración TCP/IP de cada activo informático se hará de manera manual, distribuyendo un número consecutivo por cada computadora.

Artículo 17: El nombre con que la computadora se integra al dominio UCI debe tener el sufijo CICPC para diferenciarlas de las demás computadoras.

2.3.2.2- Control de uso de los recursos y de la información.

Se considera recurso del Proyecto CICPC las computadoras, quemador de DVD, scanner e impresora, así como se entiende por información a todos los fichero, documentos y programas que contengan datos sobre el proyecto o que se utilicen para la implementación del mismo.

Artículo 18: La información Confidencial que se encuentre en formato duro, debe estar bajo algún tipo de seguridad y bajo la responsabilidad de algún miembro del consejo técnico de dirección del proyecto.

Artículo 19: Se prohíbe tener copias digitales de información confidencial en otras computadoras que no sean las del laboratorio del proyecto o portátiles autorizadas por el proyecto.

Artículo 20: Está prohibido divulgar o mostrar cualquier tipo de información clasificada como confidencial a personas ajenas al mismo.

Artículo 21: El Jefe del Proyecto es la única persona que puede autorizar por necesidades del proyecto la divulgación de algún tipo de información clasificada como Confidencial.

Artículo 22: Está prohibido compartir información confidencial o cualquier tipo de información a menos que sea para uso inmediato e internamente en el laboratorio con los permisos correspondientes.

Artículo 23: Se prohíbe la entrada al laboratorio a cualquier persona que no pertenezca a la plantilla del proyecto, a excepción de que cuente con la autorización del Jefe del Proyecto o de algún miembro del consejo técnico; dicha autorización deberá ser un documento donde se especifique el nombre de la persona(s) que se debe autorizar y lleve el nombre y la firma del que autoriza. (**Ver Anexo 6**).

Artículo 24: Se prohíbe el acceso a las computadoras a personas ajenas al Proyecto CICPC.

Artículo 25: Está prohibido utilizar el acceso remoto a cualquier computadora del laboratorio desde fuera del mismo.

Artículo 26: Está prohibido enviar por correo electrónico información clasificada como confidencial a cuentas de correo externas al dominio UCI.CU. En caso de que sea estrictamente necesario dicha información debe ir compactada y cifrada con el algoritmo de encriptación seleccionado en la Universidad.

Artículo 27: La cuenta de administración local de las computadoras del laboratorio y la del BIOS de la computadora solo deben conocerla los administradores de sistemas y los miembros del consejo técnico de dirección del proyecto.

Artículo 28: Toda la información clasificada como confidencial debe tener copia de seguridad en el servidor central de producción.

2.3.2.3- Medidas que garantizan la integridad de la información.

Artículo 29: Se prohíbe la modificación de los grupos de usuarios implantados en los ambientes de desarrollo.

Artículo 30: Se prohíbe la manipulación o transformación del ambiente de desarrollo implementado en la computadora.

Artículo 31: Los administradores de sistema del proyecto serán los responsables de garantizar el soporte y mantenimiento del hardware y el software necesarios para garantizar la producción en los laboratorios del proyecto.

Artículo 32: Se prohíbe la creación de cuentas de usuarios locales en los ambientes de desarrollo.

Artículo 33: Las cuentas locales: administrador e invitados deberán estar en todo momento deshabilitadas.

Artículo 34: Se prohíbe la modificación o eliminación de la cuenta local sysadmin presente en las computadoras del proyecto.

Artículo 35: Cuando una computadora necesite un nuevo programa, o tenga problemas tanto en hardware como en software es responsabilidad del usuario que esté trabajando en ese momento de realizar la notificación vía correo electrónico a los administradores del sistema para que pueda ser revisado y arreglado el problema.

Artículo 36: La notificación para soporte debe ser según un Modelo de Solicitud de Mantenimiento **(Ver Anexo 7)**.

Artículo 37: Los administradores del sistema deben dar respuesta a la solicitud en veinte y cuatro (24) horas, aunque en el caso de problemas de hardware puede demorarse mucho más tiempo ya que depende de factores externos al proyecto.

Artículo 38: Los administradores del sistema deben llevar un control de las solicitudes que han recibido, y el estado de respuesta de las mismas (no resuelta, resuelta, en proceso, esperando por otra persona, aplazada).

Artículo 39: Un administrador de sistema puede interrumpir el trabajo del usuario que tiene planificado tiempo de máquina para arreglar el problema, si la interrupción se puede clasificar como breve, en caso contrario debe esperar a los horarios entre los turnos de trabajo (12 – 2 PM y 6 – 8 PM).

Artículo 40: Los administradores de sistema son los responsables de que cada computadora tenga un antivirus y que el mismo este actualizado.

Artículo 41: Está prohibido el intercambio de códigos malignos entre las personas del proyecto.

Artículo 42: Es responsabilidad de los administradores de sistema hacer revisiones cada 15 días a las tecnologías informáticas del proyecto.

2.3.2.4- Seguridad y uso correcto de los medios.

Artículo 43: Toda persona que haga uso de los medios del laboratorio deberá protegerlo de daños casuales e intencionales, tanto el hardware como el software, siendo el responsable directo de los mismos mientras dure su tiempo de computadora.

Artículo 44: En los horarios de trabajo hay que mantener un adecuado silencio para que no se afecte la concentración de los demás usuarios.

Artículo 45: Se prohíbe fumar, comer o ingerir bebidas dentro del laboratorio en cualquier momento.

Artículo 46: Debe utilizarse una correcta vestimenta y un correcto vocabulario dentro del laboratorio en todo momento. Una correcta vestimenta implica entre otras cosas el no uso de chancletas de baño, pantalones cortos, camisetas, blusas muy cortas, o gorras.

Artículo 47: Las consolas de aire acondicionado, de no tener daños, deben estar conectadas a 3 temperaturas: 18, 20 y 22 para garantizar el cuidado de las computadoras.

Artículo 48: El laboratorio debe cerrarse de 6:00 a 8:00AM para el recibimiento y entrega de los turnos de guardia; y media hora todos los días para actividades de limpieza, siendo esta la responsabilidad de las auxiliares del docente.

Artículo 49: Cuando sea necesario mover sillas para otros puestos, estas deben ser devueltas a su posición inicial inmediatamente después de que el usuario que las movió termine de usarla, y se debe evitar a toda costa el recostarse fuertemente de ellas, ya que son muy débiles y se rompen con facilidad.

Artículo 50: En caso de lluvia se prohíbe usar el laboratorio a menos que se garantice una forma de limpiarse los pies antes de entrar al mismo; y en caso de penetración del agua por las puertas de los balcones, se deben apagar inmediatamente todos los equipos y cerrar el local.

Artículo 51: Se prohíbe marcar o pintar cualquier medio de trabajo, en cualquier caso pudiera emplearse pegatinas u otros adhesivos fácilmente removibles y que no dejen marca en los equipos.

2.3.2.5- Control del uso, traslado y entrada de tecnologías de la información.

Artículo 52: Los soportes magnéticos que contienen información, sistemas y/o, programas de aplicación pertenecientes al Proyecto CICPC solo pueden introducirse y/o extraerse con la anuencia del Jefe del Proyecto y el Jefe de Seguridad, y dejar constancia escrita en un Registro de soportes magnéticos (**Ver Anexo 8**) habilitado al respecto.

Artículo 53: Para utilizar soportes de propiedad personal o de otra entidad será necesario contar con la autorización del Jefe de Seguridad, debiendo ser revisados contra virus informáticos u otros programas dañinos.

Artículo 54: Al solicitarse y entregarse los soportes magnéticos a los trabajadores se asentarán en el Registro de Entrega/Recepción (**Ver Anexo 9**). Al ser devueltos los soportes magnéticos se revisarán contra virus informáticos y después se hará constar la devolución en el Registro.

Artículo 55: Cualquier movimiento, traslado de las tecnologías informáticas fuera del local para una reparación o por cualquier eventualidad, debidamente autorizada se anotara en el Libro de Incidencias (**Ver Anexo 5**). Aclarando en observaciones motivos y hacia dónde va, así como todos los datos de la persona que traslade el equipo y quede bajo su custodia, por parte de contabilidad se hará el movimiento de tarjeta de medio básico.

2.3.3- Contratos a terceros.

Artículo 56: Se solicita a la dirección de laboratorio del docente 5, los servicios de un técnico de laboratorio, el cual debe trabajar en turnos de nueve (9) horas, desde las 8:00 AM hasta 5:00 PM.

Artículo 57: La dirección del laboratorio deberá mantener constancia entre los técnicos que presten el servicio, tratando de que sean siempre los mismos.

Artículo 58: La dirección del proyecto puede solicitar la imposición de una medida disciplinaria del técnico asignado en caso de que este no cumpla con los servicios que se solicitan.

Artículo 59: Para ayudar en el control del técnico, la dirección del proyecto facilitará un listado actualizado de la plantilla del proyecto, pondrá identificación visible en todas las computadoras, el inventario de medios existentes, el nombre de todas las personas que pertenecen al consejo técnico de dirección del proyecto, y el listado de estudiantes que deberán sustituir al técnico a partir de las 5:00 PM en la guardia nocturna.

Artículo 60: Para ayudar al trabajo del técnico la dirección del proyecto pondrá a su disposición una computadora.

Artículo 61: La dirección del proyecto entregará una planilla de control de guardia que debe ser llenada por todas las personas que realicen la guardia en las veinte y dos (22) horas del día.

Artículo 62: Se concibe que dada la posición de persona externa al proyecto, el técnico utilice un lenguaje correcto y respetuoso con todos los integrantes del proyecto; incluso cuando este llamando la atención por algo que este reglamentado en este documento.

Artículo 63: El técnico será responsable directo de todos los medios que existan en el laboratorio en el momento en que inició su horario de guardia, y será el guardián de la llave del laboratorio durante el periodo de tiempo que dure la misma.

2.3.3.1- Inicio de la guardia.

Artículo 64: Al comenzar su turno de guardia, deberá dejar su nombre y firmar en la planilla de control de guardia, indicando si recibe “conforme” el laboratorio, y en caso negativo apuntar como incidencia su no conformidad.

Artículo 65: Deberá informar a la dirección de los laboratorios los medios que necesitan mantenimiento o sustitución por encontrarse rotos o fuera de servicio (como sillas, mesas, aire acondicionado, ventanas, puertas, o medios tecnológicos).

2.3.3.2- Durante la guardia.

Artículo 66: El responsable de guardia, deberá garantizar que solo entren al laboratorio las personas que pertenezcan al proyecto, según la plantilla entregada; o que cuenten con la autorización directa de algún miembro del consejo técnico o del Jefe del Proyecto, según lo estipulado en el artículo 23.

Artículo 67: El técnico o el responsable de guardia podrán solicitar algún tipo de identificación para confirmar si la persona que está tratando de acceder al laboratorio es quien dice ser.

Artículo 68: En caso de que alguna persona externa al proyecto necesite hablar con alguien que se encuentre trabajando dentro del laboratorio, el técnico deberá localizarle para que pueda salir a atender a su visita, lo cual debe hacer tratando de no molestar el ambiente de trabajo.

Artículo 69: Deberá garantizar que las consolas de aire acondicionado, de no tener daños, estén a temperaturas: 18, 20 y 22. Según lo estipulado en el artículo 47, y que la puerta permanezca cerrada para mantener el mismo.

Artículo 70: Deberá testear la red en busca de carpetas compartidas, notificando inmediatamente al Jefe del Proyecto cuando encuentre alguna información que parezca ser del proyecto.

Artículo 71: Deberá testear el contenido de la información en las computadoras del proyecto, borrando aquella que identifique como juegos, películas, videos, o pornografía.

Esta actividad debe ser realizada cuando nadie esté trabajando en la computadora testeada.

Artículo 72: Deberá testear los componentes de hardware en las computadoras del proyecto, informando inmediatamente si detecta algún faltante. Esta actividad debe ser realizada cuando nadie esté trabajando en la computadora testeada.

Artículo 73: Deberá exigir que todo el estudiante del proyecto que ingrese a trabajar deje su bolso, mochila, carpeta u otro accesorio en el que puede caber algún componente tecnológico en la parte delantera del laboratorio.

Artículo 74: Deberá intervenir en caso de que observe a algún miembro del proyecto tratando descuidadamente un medio tecnológico, rompiendo en sello de la unidad central de las computadoras o tratando de arreglar por su cuenta algún dispositivo externo.

Artículo 75: Deberá garantizar que ningún miembro del proyecto introduzca algún medio tecnológico que no esté debidamente autorizado por la dirección del proyecto. El único medio propio que se autoriza es la entrada de audífonos, y medios de almacenamiento como CD, Flash y Disco 3 ½.

Artículo 76: Deberá impedir que cualquier persona, sea interna o externa al proyecto saque algún medio (o parte de este) sin el conocimiento y autorización directa del jefe del proyecto.

Artículo 77: Deberá llamar la atención de aquel que en horario de tiempo de máquina este jugando, viendo películas, series o cualquier otro entretenimiento que no corresponda con el horario de trabajo.

Artículo 78: Deberá hacer llamado de atención a cualquier persona que esté afectando con su actuar la limpieza, el orden o el silencio del laboratorio.

Artículo 79: Deberá cuidar que el horario de limpieza se realice en el momento en que está establecido y que ningún auxiliar de limpieza extraiga del laboratorio algo más que suciedad.

Artículo 80: Si en algún momento el fluido eléctrico falla, pasados los primeros cinco (5) minutos. El técnico deberá verificar que todas las computadoras y los backups queden apagados. Y cuando el fluido se restablezca deberá proceder a abrir el laboratorio comprobando nuevamente el hardware y el software instalado.

Artículo 81: El técnico puede ser reemplazado durante el tiempo que lo necesite, siempre y cuando garantice que los servicios solicitados no se afecten, y se deje constancia del reemplazo en el libro de guardia.

Artículo 82: Durante el horario establecido para el almuerzo: de 12:00 a 1:00 PM, el técnico podrá solicitar el apoyo de algún miembro del consejo técnico que se encuentre trabajando para que asuma la responsabilidad sobre el laboratorio durante la hora que él se encuentre ausente; nunca puede dejar el laboratorio sin alguien responsable de garantizar la seguridad del mismo.

Artículo 83: El técnico puede cerrar el laboratorio del proyecto cuando este quede vacío; y tiene la obligación de reabrirlo si cualquier miembro del proyecto necesita entrar.

Artículo 84: Al finalizar el turno de guardia el técnico deberá dejar al estudiante que realizará el turno de noche la planilla de control de guardia, para que este continúe registrando las incidencias que ocurran después de las 5:00 PM.

Artículo 85: Si al finalizar el turno de guardia del técnico, el estudiante que realizará la guardia nocturna, no se ha presentado debe cerrar el laboratorio a menos de que alguien del consejo técnico se responsabilice por él.

2.3.3.3- Final de la guardia.

Artículo 86: En el horario de 6:00 AM a 8:00 AM debe hacerse un recuento completo de los medios, y dejarse constancia en la planilla de control de guardia de cualquier cosa que falte.

Artículo 87: En ese horario debe organizarse meticulosamente el laboratorio, ubicando las computadoras, sillas, mesas, y demás mobiliarios en el lugar que le corresponde y según la organización imperante.

2.3.4- Guardia estudiantil en el turno de noche.

Artículo 88: Se implementará un horario de guardia nocturna con los estudiantes del proyecto a partir de las 5:00 PM para garantizar la continuidad de todos los servicios que se prestaban de 8:00 AM a 5:00 PM.

Artículo 89: La guardia nocturna se realizará en dos turnos, estando 1 estudiante al frente de cada uno:

- 1er Turno: 5:00 PM – 12:00 AM
- 2do Turno: 12:00 AM – 6:00 AM

Artículo 90: La guardia nocturna estará apoyada por un técnico de la dirección de laboratorio que permanecerá de guardia en el piso de docente, y al cual puede acudirse en caso de que se necesite.

Artículo 91: La guardia será publicada a toda la plantilla del proyecto, los sábados de cada semana (al mismo tiempo que se publique el tiempo de máquina de la semana siguiente), e incluirá los afectados desde el domingo hasta el sábado siguiente.

Artículo 92: Un estudiante puede cambiar el turno de guardia con otro, siempre que se notifique a la planificadora, yendo personalmente a verla los 2 estudiantes que realizarán el cambio.

Artículo 93: El estudiante será responsable directo de todos los medios que existan en el laboratorio en el momento en que inicie su horario de guardia hasta que haga entrega de la misma.

Artículo 94: El estudiante que incumpla con su horario de guardia será amonestado dejando constancia en el expediente del proyecto y se le planificará nuevamente la guardia para la semana siguiente.

2.3.5- Sanciones disciplinarias.

2.3.5.1- Disposiciones generales.

Artículo 81: Las posibles faltas cometidas en referencia con lo dispuesto en el reglamento descrito en este documento pueden clasificarse en:

a) Leves

b) Graves

c) Muy Graves

2.3.5.2- Faltas Leves.

Artículo 82: Se consideran faltas leves la violación de lo establecido en los artículos 3, 4, 6, 15, 16, 17, 21, 28, 29, 30, 31, 32, 33, 35, 37, 39, 40, 43, 48, 50, 57, 63, 75.

Artículo 83: Una falta de carácter leve debe ser atendida con un llamado de atención inmediato y hay que dejar constancia de que fue amonestado, puede ser informando a su jefe inmediato superior, o al jefe del proyecto, o dejando constancia escrita en el informe de la guardia.

Artículo 84: Si el infractor incurre repetidamente en faltas de carácter leve, demostrando su incapacidad para regirse por las reglas más básicas, deberá ser amonestado en privado por su jefe inmediato y el jefe del proyecto, dejando constancia de su amonestación en el expediente del proyecto que tiene cada estudiante.

2.3.5.3- Faltas Graves.

Artículo 85: Se consideran faltas graves la violación de lo establecido en los artículos 10, 11, 13, 14, 18, 20, 22, 24, 25, 26, 56, 61, 80.

Artículo 86: Una falta de carácter grave debe ser notificada al jefe inmediato del infractor, el cual debe aplicar una medida disciplinaria que puede ser:

a) Amonestación privada frente a su jefe inmediato y el jefe del proyecto, dejando constancia de su amonestación en el expediente del proyecto que tiene cada estudiante.

b) Amonestación pública frente al resto de los integrantes del proyecto, dejando constancia de su amonestación en el expediente del proyecto que tiene cada estudiante.

c) Amonestación y análisis en el Comité de Base (si es militante), dejando constancia de la amonestación en su expediente del militante.

d) Prohibición de entrar al laboratorio del proyecto por un determinado tiempo en dependencia de las consecuencias de sus actos.

2.3.5.4- Faltas muy Graves.

Artículo 87: Se consideran faltas muy graves la violación de lo establecido en los artículos: 12, 27, 41, 49, 57, 62.

Artículo 88: Una falta de carácter muy grave debe ser notificada al jefe de proyecto, el cual debe aplicar una medida disciplinaria que puede ser:

a) Separación inmediata del proyecto con su correspondiente notificación escrita en el expediente del estudiante o del profesor en dependencia del caso.

2.4- Conclusiones.

En este capítulo se expusieron las tablas para el análisis de riesgos de los activos informáticos con que cuenta el Proyecto CICPC, además se presenta el reglamento que conforma el Plan de Seguridad Informática y las sanciones disciplinarias que se deben imponer al personal que viole alguno de estos artículos.

CAPÍTULO 3

ESTRATEGIA DE ADMINISTRACIÓN Y CONFIGURACIÓN DEL ENTORNO CONTROLADO DE DESARROLLO

3.1- Introducción.

En este capítulo se presentan las características que presenta el Entorno del Proyecto CICPC, se brinda una descripción para la base del ambiente de producción, se dan a conocer los criterios a tener en cuenta para la configuración del Entorno Controlado de Desarrollo, además de explicar los distintos procedimientos para la creación, mantenimiento y actualización del software y hardware.

3.2- Características del Entorno.

3.2.1- Hardware.

Las características de hardware que presentan las computadoras del Proyecto CICPC son las siguientes:

Placa Base o Motheboard	
Tipo de procesador	Intel Pentium 4, 3000 MHz
Memoria del sistema	1015 MB (2 memorias de 512 MB).
Tipo de BIOS	AMI del 24/6/2005
Fabricante	AsusTek Computer Inc
Producto	P5GD1-HVM
Monitor	
Tarjeta gráfica	(R) 82915G Express Chipset Family (128 MB) onboard
Acelerador 3D	Intel GMA 900
Monitor	15'' CRT
Multimedia	
Tarjeta de sonido	Realtek ALC880(D) @ Intel 82801FB ICH6 - High Definition Audio Controller [B-1]
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	ST380817AS (80 GB, 7200 RPM, SATA)
Lector óptico	HL-DT-ST DVD-ROM GDR8163B (16x/52x DVD-ROM)
Tamaño real del disco duro	76316 MB
Red	
Tarjeta de red	(R) PRO/1000 MT Network Connection

Figura 1: Características de hardware

3.2.2- Organizacionales.

El trabajo está estructurado por Grupos de Trabajo según los roles con que cuenta el Proyecto CICPC actualmente para la producción, los mismos se identifican en:

- Analistas.
- Diseñadores – Programadores.
- Arquitectos.
- Arquitectos de información.
- Diseñadores y Programadores Base de datos.
- Manual de Usuario.
- Montadores de Interfaz de Usuario.
- Gestión de proyectos.
- Calidad.
- Portal Web.

Cada Grupo de Trabajo necesita un "Ambiente de Desarrollo" específico para realizar sus funciones en el proceso de desarrollo del software, dicho entorno se define en dependencia de las herramientas que se necesitan para la realización de los aplicativos, y pueden ser generalizados para varios Grupos de Trabajo, obteniendo como resultado las siguientes formas:

- Base:
    - Manuales de usuario, Calidad, Arquitectura de la información, Gestión de proyectos.
- Analistas.
- Arquitectos.
- Base de datos.
- Portal Web.
- Programadores, Montadores de Interfaz de Usuario.

El "Ambiente de Desarrollo", desde el punto de vista conceptual, no es más que la creación de una "Imagen" que es almacenada y ejecutada en dependencia del grupo de trabajo que lo necesite.

¿Qué es una Imagen?

Una Imagen no es más que copiar toda la información que se incluye en el disco o partición: ficheros de sistema, carpetas, documentos, configuraciones, programas, es decir, realizar

una copia idéntica del original, de tal manera que en caso de ocurrir un desastre poder restaurarla y dejar el sistema exactamente igual que en el momento de crearla.

3.2.3- Software.

A partir del levantamiento de las herramientas necesarias para el desarrollo del Proyecto CICPC se reúne la siguiente información:

Tabla 6: Herramientas presentes en las imágenes.

Grupo de Trabajo	Herramientas	Versión
Base	Sistema Operativo Windows	XP Service Pack 2
	Paquete de Microsoft Office	2003
	TortoiseSVN	1.4.1
	Máquina virtual de java	1.5
	Drivers de la tarjeta madre	Asus P5GD1-HVM
	Códecs	
	Adobe Acrobat	8.0 Pro
	Ad-Aware Professional	6
	Winrar	3.71
	Antikeylogger Killer	1.5
	Norton Ghost Corporate Edition Client	8
	VMWare Workstation	5.5.1
	Kaspersky Antivirus	6
	Babylon Translator	6
	Mozilla Firefox	2.0.0.12
	Beyond Compare	2.2.7
	Total Commander Ultimate Prime	3.1
	RoboHelp	
Analistas	Visual Paradigm	3
Arquitectos	Apache Tomcat	6.0.14
	Eclipse	3.3
	Exadel Studio	4.0.1
	Red Hat Developer Studio RC	1
	Gestor de base de datos Postgres	8.2.4-1
	Gestor de base de datos MySQL	5.0.47
	Visual Paradigm	3
	Erwin Studio	7

	PLSQL Developer	7.1
	Aptana	
Base de datos	PLSQL Developer	7.1
	Gestor de base de datos Postgres	8.2.4-1
	Erwin Studio	7.0
	Instant Client	
Portal Web	Apache HTTP Server	2.2.3
	Gestor de base de datos MySQL	5.0.47
	PHP	5.2.1
	Enterprise Manager System	3.4.04
	NuSphere	4.6.3
	HtmlEditor	
Programadores	Apache Tomcat	6.0.14
	Eclipse	3.3
	Exadel Studio	4.0.1
	Gestor de base de datos Postgres	8.2.4-1
	Visual Paradigm	3
	PLSQL Developer	7.1

Por la importancia que revisten las herramientas anteriormente reflejadas en la tabla para el desarrollo de los aplicativos, se presenta una breve explicación de las mismas.

Características de las herramientas escogidas.

Office.

Microsoft Office es una suite ofimática desarrollada por la empresa Microsoft [Office].

- **Microsoft Word:** procesador de texto.
- **Excel:** es un programa de hoja o planilla de cálculo.
- **Outlook:** es un administrador de información personal y un complejo cliente de correo electrónico.
- **PowerPoint:** es un muy popular programa para desarrollar y desplegar presentaciones visuales.
- **Visio:** software de dibujo vectorial

TortoiseSVN.

TortoiseSVN es un cliente gratuito de código abierto para el sistema de control de versiones Subversion, TortoiseSVN maneja ficheros y directorios a lo largo del tiempo, Esto permite

que pueda recuperar versiones antiguas de sus ficheros y examinar la historia de cuándo y cómo cambiaron sus datos, y quién hizo el cambio [TortoiseSVN].

Máquina Virtual de Java.

Una Máquina virtual Java (en inglés *Java Virtual Machine*, JVM) es un programa nativo, es decir, ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en un código binario especial, el cual es generado por el compilador del lenguaje Java [JVM].

Adobe Acrobat Reader.

Adobe Reader es una aplicación que permite visualizar e imprimir archivos en formato PDF [AcrobatReader].

AD-Aware.

Ad-Aware analiza la computadora en busca de ficheros "espía" y ayuda a eliminarlos de forma rápida y segura; detecta y elimina spywares, dialers, troyanos, realiza minería de datos, agressive advertising, parásitos, scumwares, secuestradores de navegador, y cookies de seguimiento [AD-Aware].

WinRAR.

WinRAR es un potente programa compresor y descompresor de datos multifunción, una herramienta indispensable para ahorrar espacio de almacenamiento y tiempo de transmisión al enviar y recibir archivos a través de Internet o al realizar copias de seguridad.

AntiKeylogger.

AntiKeylogger es de los primeros programas en ofrecer una protección contra programas espía que registran las pulsaciones del teclado. De similar forma a como pasa con los antivirus.

Norton Ghost.

Es la herramienta de creación de imágenes, implementación y administración corporativa, incluye una función sencilla de creación de imágenes e implementación, y migración de datos del SO y de la configuración del usuario, distribución de software, inventario de software y hardware, y retirado seguro de sistemas [NortonGhost].

VMWare Workstation.

Es uno de los más utilizados pues permite la emulación en plataformas PC x86, esto permite que cualquier usuario con una computadora de escritorio o laptop pueda emular tantas máquinas virtuales como los recursos de hardware lo permitan.

Kaspersky.

Brinda una protección a gran escala a la computadora basada en Windows, incorpora mecanismos de seguridad, como el bloqueo de comportamiento y el chequeo de integridad que no requieren de la actualización de las bases de antivirus [Kaspersky].

Babylon Translator.

Traduce palabras y expresiones del inglés a 12 idiomas, funciona minimizado en forma de ícono en la barra de tareas, y basta con seleccionar una palabra en inglés para obtener su traducción. Una vez hecho eso, nos permite buscar su significado en varios diccionarios disponibles en Internet, y si se trata de una palabra nueva, nos permite añadirla al diccionario de traducción.

Mozilla Firefox.

Es un navegador de Internet, con interfaz gráfica de usuario. El programa es multiplataforma y está disponible en versiones para Microsoft Windows, Mac OS X y GNU/Linux. El código ha sido portado por terceros a FreeBSD, OS/2, Solaris, SkyOS, BeOS y más recientemente, Windows XP Professional x64 Edition [Mozilla].

Beyond Compare.

Beyond Compare es una utilidad que permite localizar y sincronizar diferencias entre directorios y ficheros, puede comparar archivos de cualquier extensión, carpetas y sitios FTP, te ayuda a analizar diferencias en detalle entre dos archivos.

Total Commander.

Total Commander mejora sustancialmente el explorador de Windows. Hace funciones de cliente FTP, permite búsqueda avanzada de ficheros, comparación del contenido de varios archivos.

Robo Help.

Adobe Systems Robo Help es un aplicación informática para la creación y edición de manuales de ayuda, permite que los autores de contenidos técnicos y de ayudas y los desarrolladores de contenido web creen, gestionen y publiquen sistemas de ayuda y bases de conocimiento independientes.

Visual Paradigm.

Visual Paradigm para UML es una herramienta profesional de modelado en UML que soporta el ciclo de vida completo del desarrollo de software: análisis y diseño orientados a objetos, construcción, pruebas y despliegue. El software de modelado UML ayuda a una

más rápida construcción de aplicaciones de calidad, mejores y a un menor coste. Permite dibujar todos los tipos de diagramas de clases, código inverso, generar código desde diagramas y generar documentación [Paradigm].

Apache Tomcat.

Tomcat es un servidor web con soporte de servlets y JSPs. Incluye el compilador Jasper, que compila JSPs convirtiéndolas en servlets. El motor de servlets de Tomcat a menudo se presenta en combinación con el servidor web Apache [Tomcat].

Eclipse.

Eclipse es un "Entorno de Desarrollo" integrado de código abierto independiente de una plataforma, ha sido usada para desarrollar entornos de desarrollo integrados (del inglés IDE), como el IDE de Java llamado "*Java Development Toolkit"* (JDT) [Eclipse].

Exadel Studio.

Exadel Studio es un avanzado entorno de desarrollo de aplicaciones para el aprovechamiento de código fuente abierto, J2EE, AJAX y tecnologías dentro del entorno Eclipse, orientada a los enfoques de desarrollo con soporte para múltiples tecnologías de código abierto, incluyendo JSF, Struts, Hibernate, MyFaces, Oracle ADF, Shale, primavera, y otros [Exadel].

RED HAT Developer Studio Release Candidate 1.

Conjunto de plugins para Eclipse que surge, principalmente, de la fusión de JBoss IDE y Exadel Studio. Presenta mejoras en el desarrollo JSF, especialmente con la integración de las librerías para Ajax RichFaces y Ajax4JSF [RedHat].

PostgreSQL.

PostgreSQL es un servidor de base de datos relacional orientada a objetos de software libre, liberado bajo la licencia BSD [Postgre].

MYSQL.

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones, cumple con el estándar SQL, pero sin sacrificar velocidad, fiabilidad o usabilidad [MySQL].

ERWIN Studio.

ER / Studio es la arquitectura de datos y diseño de bases de datos de software. Funciona a través de múltiples plataformas de base de datos y es usado por los arquitectos de datos, modelado de datos, base de datos de los administradores y analistas de negocios para

crear y gestionar bases de datos diseños, documentar y reutilizar los activos de datos [Erwin].

Instant Client.

Instant Client le permite ejecutar sus aplicaciones sin necesidad de instalar el estándar de Oracle cliente o que tenga un ORACLE_HOME. OCI, OCCI, ODBC, JDBC y aplicaciones de trabajo sin modificación [InstClient].

PLSQL Developer.

Una herramienta para desarrollar, probar debugging y optimizar unidades de programa almacenadas de Oracle Databases. PL/SQL Developer es fácil de usar y pretende ofrecer código y rendimiento de muy buena calidad - puntos claves para el desarrollo de aplicaciones en Oracle [PLSQL].

APTANA.

Aptana es compilador de código JavaScript dirigido hacia las aplicaciones web escritas en Ajax/JavaScript. Está basado en Eclipse y lo podremos encontrar para las tres plataformas mayoritarias (Windows, Mac y Linux), ya sea como plugins del mismo Eclipse, o como aplicación por separado [Aptana].

Apache HTTP Server.

Es una herramienta se publicación de aplicaciones desarrolladas sobre tecnología Web, es un software (libre) de código abierto para plataformas Unix, Windows, Macintosh y otras, que implementa el protocolo HTTP. Presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido [Apache].

PHP.

Paquete compilador del lenguaje PHP (*PHP Hypertext Preprocessor*) que es un lenguaje de programación dirigido a la creación de páginas web en el servidor, diseñado originalmente para la creación de páginas web dinámicas. Es usado principalmente en interpretación del lado del servidor, pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica [PHP].

Enterprise Manager System.

EMS Mysql Manager dispone de un conjunto de herramientas con las cuales se puede controlar un servidor mysql, construir consultas, modificar privilegios. Dispone de una

interfaz gráfica altamente intuitiva y recomendable tanto para principiantes como para usuarios más experimentados [EMS].

NuSphere PHPEd.

NuSphere PHPEd es un editor de PHP tanto para profesionales como para principiantes. Los recursos de los que dispone son los siguientes: Código de colores para php, javascript, perl, sql, html, entre otros [NuSphere].

3.3- Descripción de la base para el ambiente de producción.

La base para gestionar todo el Ambiente de Desarrollo es a partir de una "Imagen", la misma incluye:

- Las políticas de seguridad necesarias.
- Herramientas.
- La garantía de ser solo usada para el tipo de hardware del proyecto.
- La configuración para el uso de las herramientas.
- Control sobre las computadoras por parte de los administradores de sistemas.

Para la creación de este ambiente de producción se hacen necesarias las siguientes imágenes:

- Base.
- Analista.
- Arquitecto.
- Base de datos.
- Portal Web.
- Programador.

Para el trabajo con las imágenes durante el proceso de desarrollo del software, se identifican un grupo de procedimientos con el fin de garantizar que todos los Grupos de Trabajo:

- Cumplan con las políticas de seguridad expresadas en el plan de seguridad presentado en el capítulo anterior.
- Que el rendimiento de la computadora sea el más óptimo posible para el rol que desempeña.
- Que no se invierta tiempo y esfuerzo de producción en instalaciones y configuraciones de los sistemas operativos, ni las herramientas que necesitan.
- Que no inviertan esfuerzo en actividades de mantenimiento de software.
- Que se afecten mínimamente cuando ocurra una rotura de hardware.

- Cumplan con las mismas configuraciones y herramientas previstas.

3.4- Criterios a tener en cuenta para la configuración.

En el epígrafe anterior se realizó el análisis y descripción de la base para el ambiente de producción, partiendo de ese análisis el siguiente epígrafe pretende dar a conocer cuáles son los criterios a tener en cuenta para la configuración inicial de las imágenes que se van a implementar para la protección de la información y el acceso a las computadoras por el personal ajeno al proyecto. Estos criterios están en correspondencia con el plan de seguridad expuesto en el capítulo anterior.

1. **De configuración de la red.**
    - La configuración TCP/IP de los equipos de cómputos (dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas) va a ser estática, asignando un número en dependencia de su localización.
        - Los números van a ser del 1 – 30, reservando del 31 – 35 para posible contaminación de algún equipo de cómputo.
    - El nombre del equipo de cómputo debe tener incluido el prefijo CICPC para que exista distinción entre los demás equipos de cómputos del docente.
    - Los equipos de cómputo deben estar incluidos en el dominio UCI de la universidad.
    - Las actualizaciones automáticas de los equipos de cómputos deben estar desactivadas, las actualizaciones de software van a ser a través de actualizaciones de las imágenes.
2. **Del acceso al equipo de cómputo.**
    - Crear el Grupo de Usuarios CICPC a partir de la plantilla del proyecto.
    - Crear la cuenta local sysadmin con permisos administrativos para el mantenimiento de software.
    - Establecer como administrador al usuario responsable del equipo de cómputo.
    - Establecer como política de seguridad local que el acceso al equipo de cómputo solo puede ser si el usuario es administrador o pertenece al Grupo de Usuarios CICPC.
3. **Del acceso al equipo de cómputo por la red**
    - El acceso remoto de los equipos de cómputos debe estar deshabilitado.
    - Se prohíbe compartir carpetas en el equipo de cómputo sin el debido nivel de acceso.

4. **De otras configuraciones.**
    - Establecer como política de seguridad local que las cuentas administrador e invitado estén deshabilitadas.
    - Desactivar el firewall del equipo de cómputo.
    - Activar el escaneo en tiempo real del antivirus instalado en el equipo de cómputo.
    - Establecer cuotas al "Disco Local C" de 300MB para los usuarios del Grupo de Usuarios CICPC.
    - Denegar espacio en disco al usuario que exceda el límite de la cuota destinado.
    - Denegar permisos de escritura en el "Disco Local D" a los usuarios del Grupo de Usuarios CICPC.

3.5- Procedimientos.

En los epígrafes anteriores se muestran cuales son las imágenes que se van a crear para los diferentes Grupos de Trabajo existentes y las políticas de seguridad necesarias a aplicar para asegurar que se cumpla el Plan de Seguridad Informática creado para mantener la confidencialidad de la información que se maneja dentro del proyecto.

A continuación se presentan un conjunto de procedimientos para el montaje de las imágenes en las computadoras del Proyecto CICPC, así como el mantenimiento y actualización de las mismas.

3.5.1- Preparación de las imágenes.

El siguiente diagrama explica cuales son las acciones a seguir para la preparación del Entorno Controlado de Desarrollo.

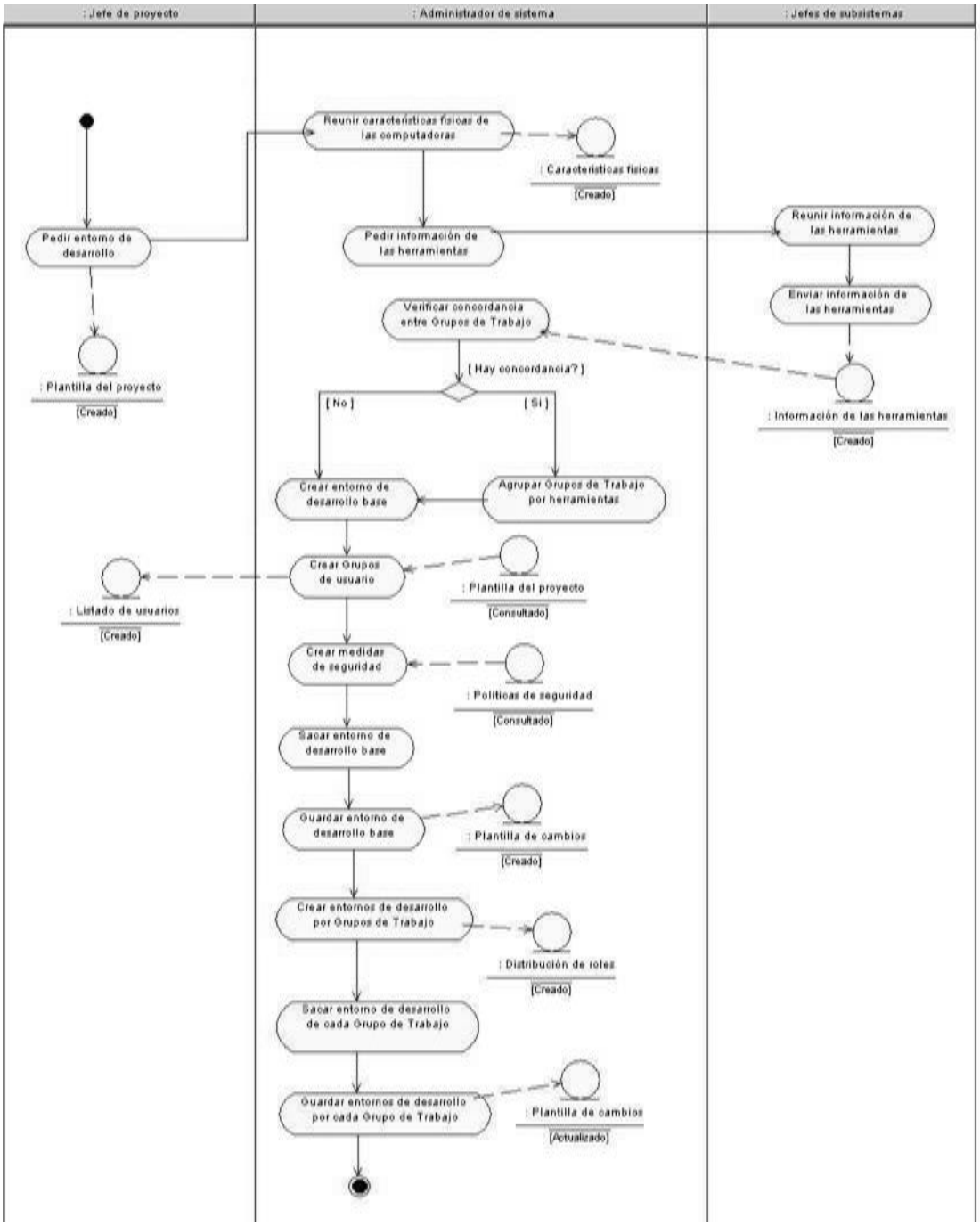

Figura 2: Preparación de las imágenes.

La comunicación entre los administradores de sistemas y los jefes de subsistemas es de vital importancia ya que los últimos son los que deciden cuales son las herramientas que se van a utilizar para el desarrollo de los aplicativos del Proyecto CICPC, si falla la comunicación entre estos conlleva a que no se instalen todo el software necesario, provocando el fracaso del Entorno Controlado de Desarrollo que se está creando.

3.5.2- Montaje de las imágenes.

El siguiente diagrama explica cuales son las actividades a seguir para el montaje de las imágenes en las computadoras de cada Grupo de Trabajo.

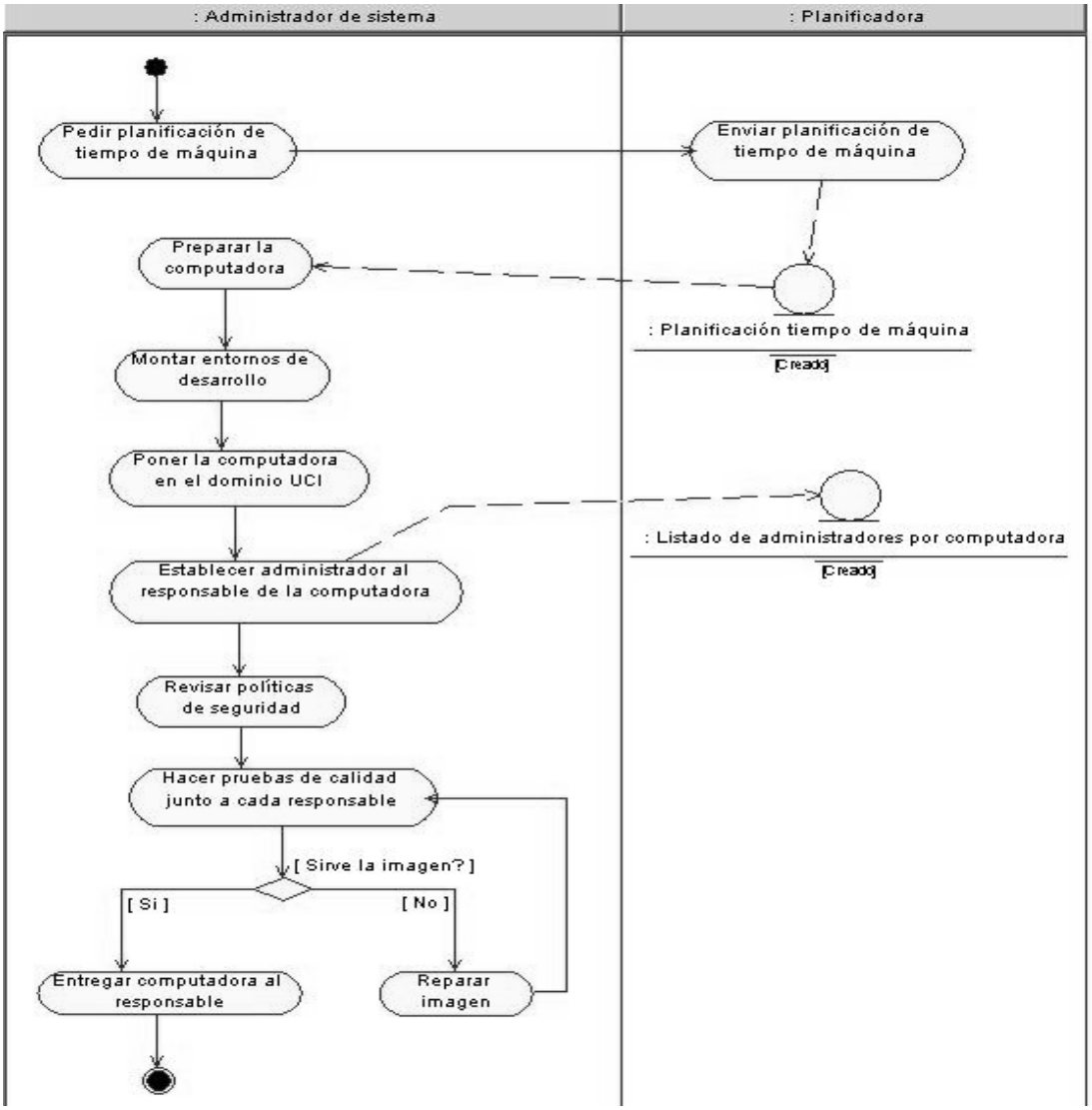

Figura 3: Montaje de las imágenes.

Lo más significante en este proceso son las pruebas de calidad que se le hacen a la imagen junto al responsable de la computadora, esto ayuda a que se detecten anomalías a tiempo y no cuando se esté en plena producción, lo cual implica a que se atrase el Grupo de Trabajo afectado.

3.5.3- Mantenimiento del hardware de la computadora.

Se entiende por mantenimiento a los pasos que se realizan cuando ocurre una rotura o cambio de algún accesorio de la computadora. El siguiente diagrama muestra cuales son las acciones a seguir cuando ocurre una rotura de hardware en alguna computadora del proyecto.

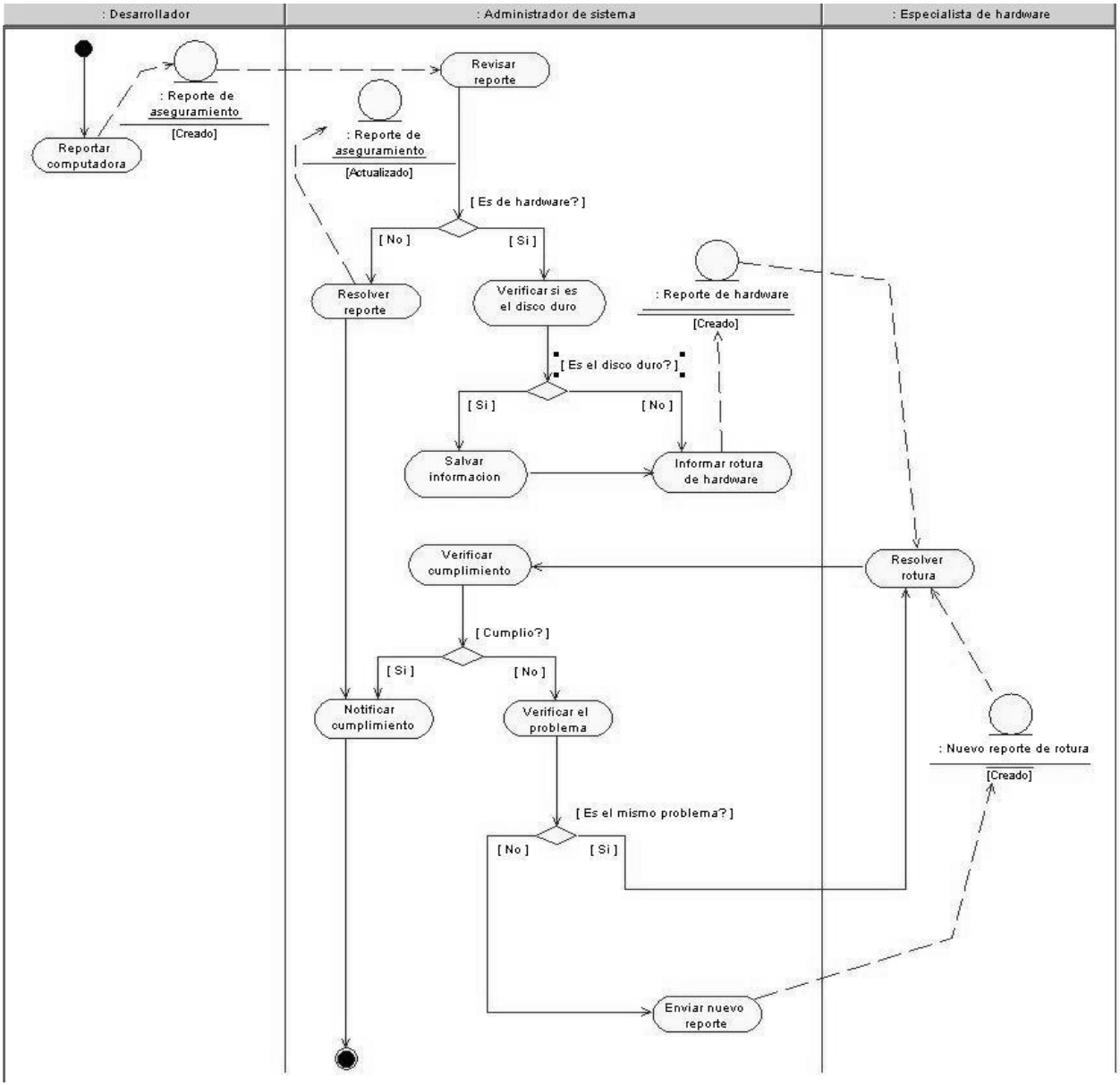

Figura 4: Mantenimiento del hardware de la computadora.

Este es uno de los principales proceso ya que la demora excesiva traerá un significado adverso a la producción.

3.5.4- Actualización del hardware de la computadora.

Se entiende por actualización de hardware los pasos necesarios para realizar un cambio de accesorio en las computadoras del proyecto. El siguiente diagrama muestra cuales son las acciones a llevar a cabo para hacer la petición de actualización de hardware.

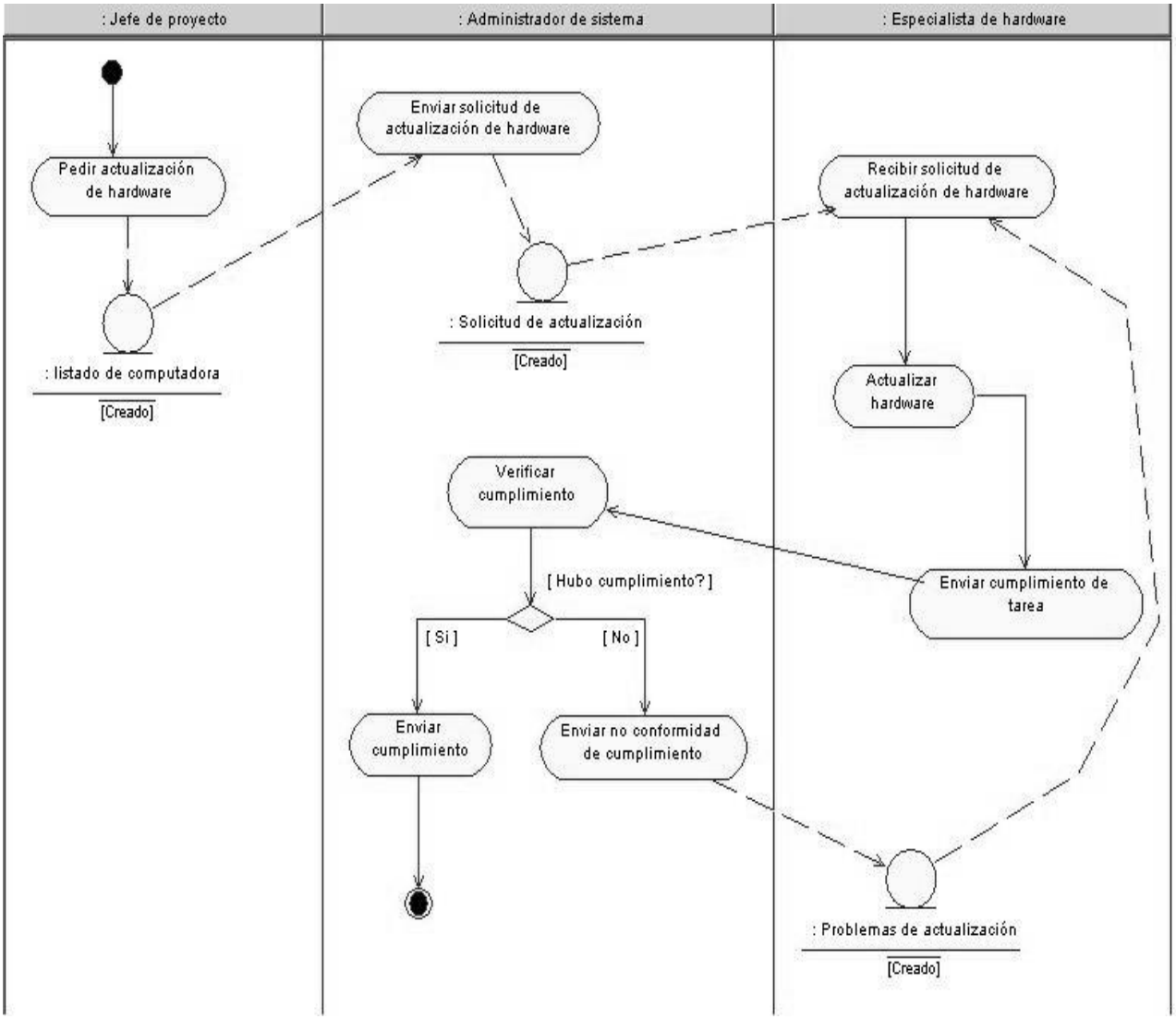

Figura 5: Actualización del hardware de la computadora.

La actualización del hardware de la computadora es de significativa importancia ya que aumenta el rendimiento de la misma, ayudando así a que el proceso productivo se incremente progresivamente.

3.5.5- Mantenimiento de software.

Se entiende por mantenimiento de software a los pasos a seguir cuando ocurre un impedimento que involucre a cualquier software instalado y configurado en la imagen en cuestión, este impedimento puede ser que el software deje de funcionar correctamente hasta una rotura de la imagen. El siguiente diagrama muestra las acciones a seguir cuando se recibe una notificación de esta índole.

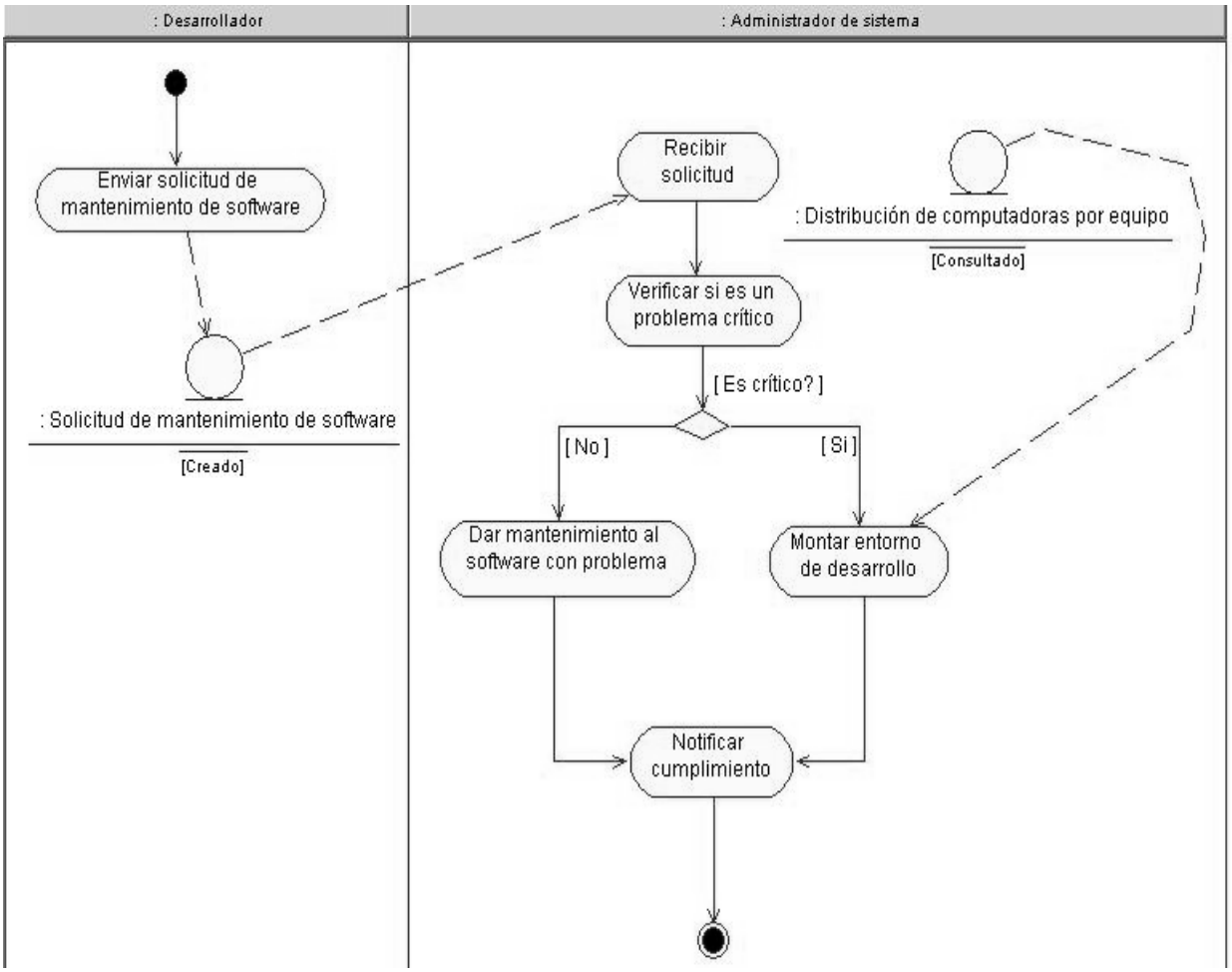

Figura 6: Mantenimiento de software.

Cuando se recibe una notificación de mantenimiento de software por parte del responsable de la computadora (en este caso es el desarrollador) se debe verificar si es un problema menor o si conlleva un nuevo montaje de la imagen.

3.5.6- Actualización de software.

Se entiende por actualización de software los pasos a seguir cuando se actualiza uno y cada uno de los software de las imágenes. En siguiente diagrama se muestra cuales son las acciones a seguir para realizar lo anteriormente descrito.

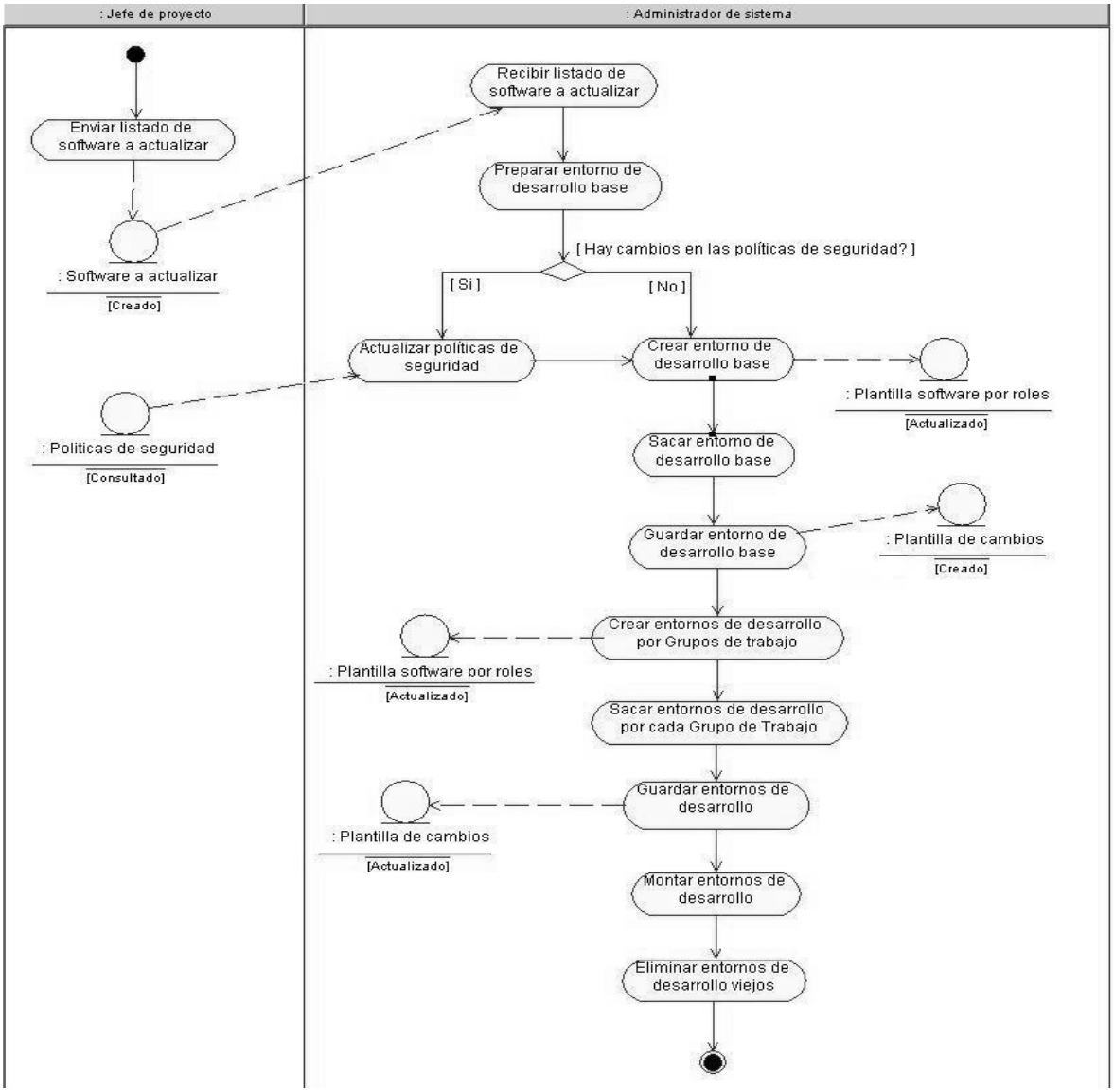

Figura 7: Actualización de software.

Este es un proceso de vital importancia ya que se debe realizar en el menor tiempo posible para afectar en lo mínimo al proceso de desarrollo de los aplicativos del proyecto.

3.5.7- Actualizar políticas de seguridad.

Se entiende por actualización de las políticas de seguridad al proceso que se realiza cuando ocurre un cambio en una o varias de las políticas descritas en el epígrafe Políticas de seguridad. El siguiente diagrama muestra cuales son los pasos para realizar las actualizaciones de las políticas de seguridad.

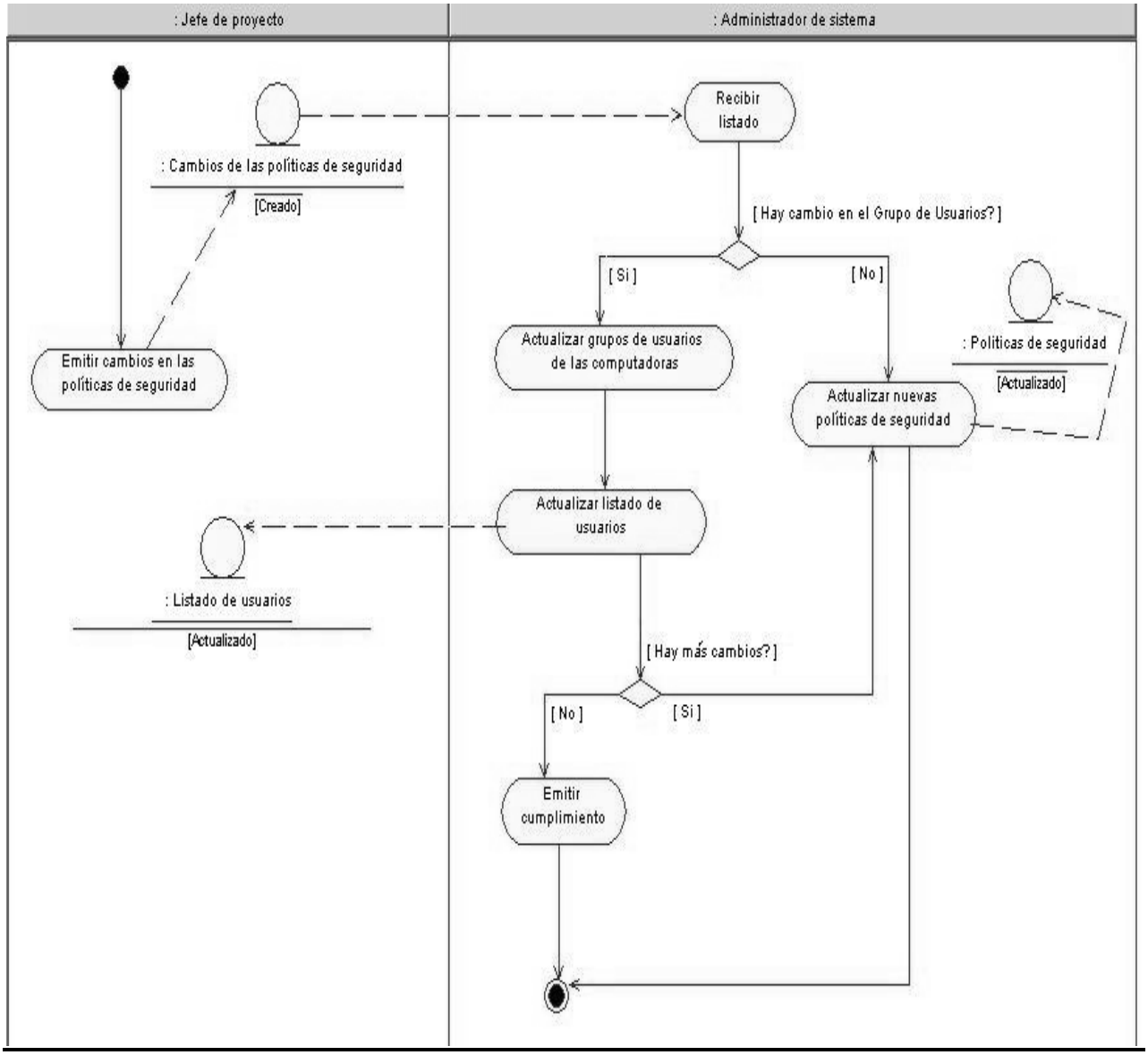

Figura 8: Actualizar políticas de seguridad.

3.5.8- Proceso de auditoría.

El proceso de auditoría consiste en agrupar y evaluar evidencias para determinar si los equipos de cómputo salvaguardan los activos, mantienen la integridad de los datos, llevan a cabo eficazmente los fines del proyecto y utilizan eficientemente los recursos. En el siguiente diagrama se muestra las acciones a seguir para realizar un proceso de auditoría.

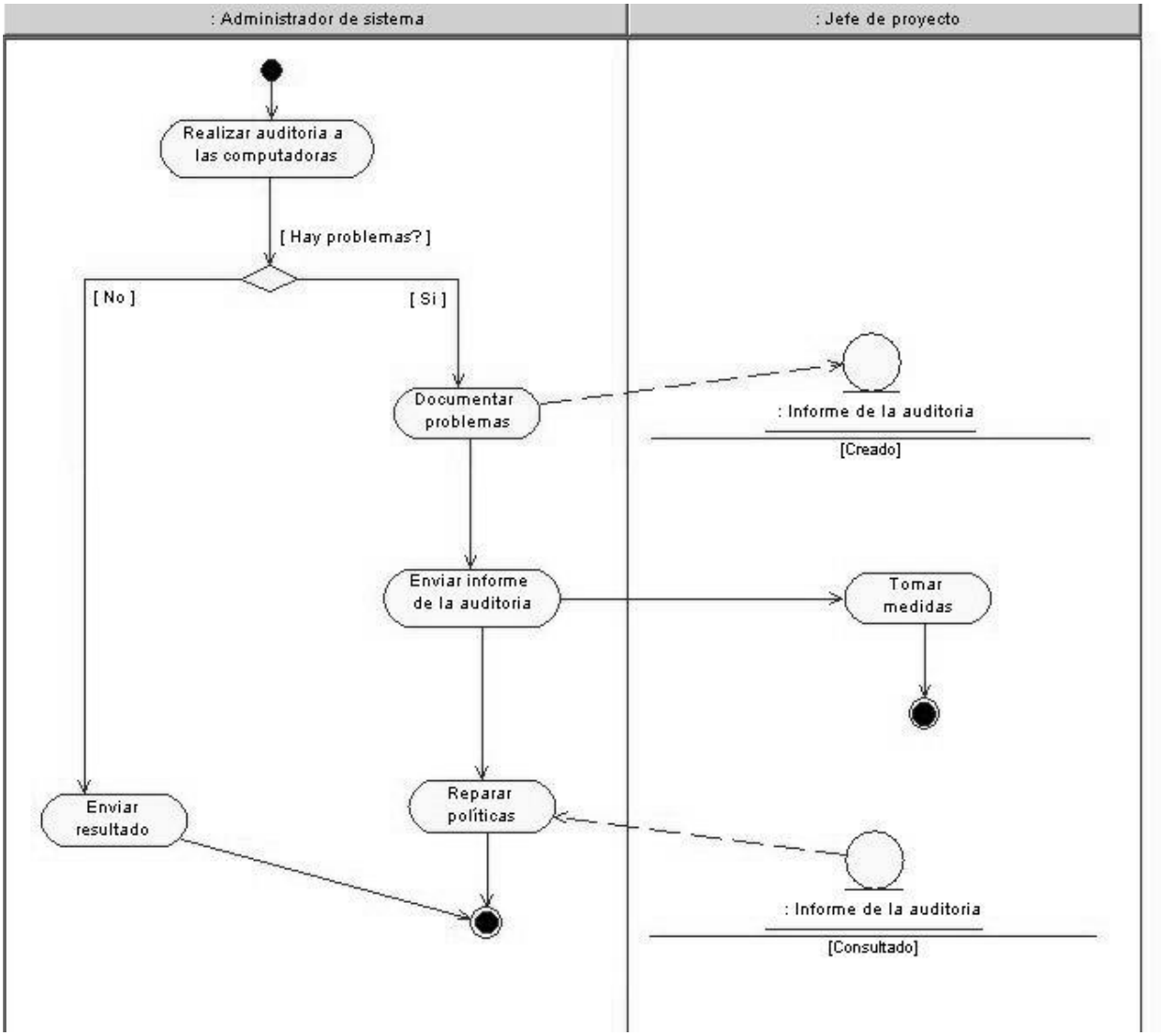

Figura 9: Proceso de auditoría.

Este es el proceso de más importancia dentro del proyecto ya que mediante él se pueden identificar amenazas contra la confidencialidad de la información y es la principal forma de comprobar el cumplimiento de las políticas de seguridad establecidas por el Plan de Seguridad para los laboratorios del proyecto. Este proceso se realiza semanalmente.

3.6- Conclusiones.

En este capítulo se definieron las características del Entorno Controlado de Desarrollo del Proyecto CICPC, así como los criterios a tener en cuenta para la configuración de los mismos. Se muestran y explican los procedimientos a llevar a cabo para la gestión del Entorno y los pasos a seguir para la realización del proceso de auditoría al cual está sujeto el proyecto semanalmente.

CAPÍTULO 4

ESTRATEGIA DE ADMINISTRACIÓN Y CONFIGURACIÓN DE LOS SERVIDORES

4.1- Introducción.

En este capítulo se presentan las características físicas que presentan los servidores del Proyecto CICPC. Se da a conocer cuáles son los servicios que se van a implementar en cada uno de los servidores, así como la selección de los sistemas operativos. También se ponen de manifiestos las políticas de seguridad para el acceso y manejo de los mismos, además de las políticas tanto de salvas como de recuperación ante cualquier tipo de falla.

4.2- Características de los servidores.

4.2.1- Hardware

El Proyecto CICPC cuenta con un número fijo de servidores, las características de hardware que presentan los mismos son las siguientes:

Servidor 1

Placa Base o Motheboard	
Tipo de procesador	Intel Pentium 4, 3000 MHz
Memoria del sistema	1015 MB (2 memorias de 512 MB).
Tipo de BIOS	AMI del 24/6/2005
Fabricante	AsusTek Computer Inc
Producto	P5GD1-HVM
Monitor	
Tarjeta gráfica	(R) 82915G Express Chipset Family (128 MB) onboard
Acelerador 3D	Intel GMA 900
Monitor	15'' CRT
Multimedia	
Tarjeta de sonido	Realtek ALC880(D) @ Intel 82801FB ICH6 - High Definition Audio Controller [B-1]
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	SST380817AS (80 GB, 7200 RPM, SATA)
Lector óptico	HL-DT-ST DVD-ROM GDR8163B (16x/52x DVD-ROM)
Tamaño real del disco duro	76316 MB
Red	
Tarjeta de red	(R) PRO/1000 MT Network Connection

Figura 10: Características físicas del servidor 1

Servidor 2

Placa Base o Motheboard	
Tipo de procesador	Intel Pentium 4 630, 3000 MHz (15 x 200)
Memoria del sistema	503 MB (DDR2-533 DDR2 SDRAM)
Tipo de BIOS	AMI (10/27/05)
Fabricante	ASUSTeK Computer INC.
Producto	P5LD2-VM
Monitor	
Tarjeta gráfica	Intel(R) 82945G Express Chipset Family (64 MB)
Acelerador 3D	Intel GMA 950
Monitor	15" CRT
Multimedia	
Tarjeta de sonido	Realtek ALC882(D) @ Intel 82801GB ICH7 - High Definition Audio Controller [A-1]
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	ST3160023AS (160 GB, 7200 RPM, SATA)
Lector óptico	ASUS DRW (DVD+RW:16x/8x, DVD-RW:16x/6x, DVD-ROM:16x, CD:40x/24x/40x)
Tamaño real del disco duro	149.0 GB
Red	
Tarjeta de red	Intel(R) PRO/1000 PM Network Connection

Figura 11: Características físicas del servidor 2

Servidor 3

Placa Base o Motheboard	
Tipo de procesador	Intel Pentium 4, 3000 MHz
Memoria del sistema	1015 MB (2 memorias de 512 MB).
Tipo de BIOS	AMI del 24/6/2005
Fabricante	AsusTek Computer Inc
Producto	P5GD1-HVM
Monitor	
Tarjeta gráfica	(R) 82915G Express Chipset Family (128 MB) onboard
Acelerador 3D	Intel GMA 900
Monitor	15'' CRT
Multimedia	
Tarjeta de sonido	Realtek ALC880(D) @ Intel 82801FB ICH6 - High Definition Audio Controller [B-1]
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	SST380817AS (160 GB, 7200 RPM, SATA)
Lector óptico	HL-DT-ST DVD-ROM GDR8163B + CD-RW
Tamaño real del disco duro	149.0 GB
Red	
Tarjeta de red	(R) PRO/1000 MT Network Connection

Figura 12: Características físicas del servidor 3

Servidor 4

Placa Base o Motheboard	
Tipo de procesador	Intel Pentium 4, 3000 MHz
Memoria del sistema	1536 MB (1 memoria de 1 GB y 1 de 512 MB)
Tipo de BIOS	AMI del 24/6/2005
Fabricante	AsusTek Computer Inc
Producto	P5GD1-HVM
Monitor	
Tarjeta gráfica	(R) 82915G Express Chipset Family (128 MB) onboard
Acelerador 3D	Intel GMA 900
Monitor	15'' CRT
Multimedia	
Tarjeta de sonido	Realtek ALC880(D) @ Intel 82801FB ICH6 - High Definition Audio Controller [B-1]
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	ST380817AS (160 GB, 7200 RPM, SATA)
Lector óptico	HL-DT-ST DVD-ROM GDR8163B + CD-RW
Tamaño real del disco duro	149.0 GB
Red	
Tarjeta de red	(R) PRO/1000 MT Network Connection

Figura 13: Características físicas del servidor 4

Servidor Integrity

Placa Base o Motheboard	
Tipo de procesador	2 procesadores Intel Itanium 2 Dual Core a 1.6GHz
Memoria del sistema	8 GB (DDR2)
Fabricante	Hewlett Packard
Producto	HPUX 11i v2
Almacenamiento	
Disquetera de 3 ½	Unidad de disquete
Disco duro	2 SAS de 2.5 de 74 GB
Lector óptico	LG DRW (DVD+RW:16x/8x, DVD-RW:16x/6x, DVD-ROM:16x, CD:40x/24x/40x)
Tamaño real del disco duro	146.0 GB
Red	
Tarjeta de red	HP PCI-X 1000Base-T Release B.11.23.0706.01

Figura 14: Características físicas del servidor Integrity

4.2.2- Servicios generales.

Los servicios generales instalados y configurados en los servidores del Proyecto CICPC son los siguientes:

- Sistema de control de versiones.
- Sistema para la gestión de proyectos.
- Sistema de compartimiento de archivos.

A continuación se presentan las características de cada uno de estos servicios.

Sistema de control de versiones.

Se llama sistema de control de versiones a la gestión de los diversos cambios que se realizan sobre los elementos de algún producto o una configuración del mismo, facilitan la administración de las distintas versiones de cada producto desarrollado, así como las posibles especializaciones realizadas [SVN].

Sistema para la gestión de proyectos.

Se llama sistema de gestión de proyecto a la disciplina de organizar y administrar recursos de manera tal que se pueda culminar todo el trabajo requerido en el proyecto dentro del alcance, el tiempo, y el costo definido.

Sistema de compartimiento de archivos.

El sistema de compartimiento de archivos permite mover uno o más archivos con seguridad entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia.

4.2.3- Servicios específicos.

Los servicios específicos instalados y configurados en los servidores del Proyecto CICPC son los siguientes:

- Sistema de integración continua.
- Sistema de modelación de base de datos.
- Sistema de publicación de aplicaciones Java.
- Sistema para la gestión de la configuración y la seguridad.
- Sistema para la gestión de los requerimientos del software.
- Sistema de publicación de aplicaciones PHP.
- Gestor de base de datos para el Portal Web.
- Gestor de base de datos para la aplicación CICPC.

Sistema de integración continua.

La integración continua es un proceso que permite comprobar continuamente que todos los cambios que lleva cada uno de los desarrolladores no producen problemas de integración con el código del resto del equipo. Los entornos de integración continua construyen el software desde el repositorio de fuentes y lo despliegan en un entorno de integración sobre el que realizar pruebas unitarias o de aceptación [IntCont].

Sistema de modelación de base de datos.

El modelado de datos es uno de los elementos más importantes a la hora de iniciar el desarrollo de cualquier proyecto. Esta es la estructura, sobre la que realmente reside la verdadera esencia de la aplicación. Incluso determina si el proyecto va a cumplir con su verdadero objetivo. Aportan la base conceptual para diseñar aplicaciones que hacen un uso intensivo de datos, así como la base formal para las herramientas y técnicas empleadas en el desarrollo y uso de sistemas de información [ModDB].

Sistema de publicación de aplicaciones Java

Los sistemas de publicación de aplicaciones Java funcionan como contenedores de servlets, son utilizados como servidor web autónomo en entornos con alto nivel de tráfico y alta disponibilidad.

Sistema para la gestión de la configuración y la seguridad.

Garantiza la continuidad operativa de su red optimizando su uso y tomando acciones proactivas antes de que ocurra un evento de falla, con el servicio de gestión y monitoreo de red se provee información en tiempo real sobre el comportamiento de su red en sus propias instalaciones.

Sistema para la gestión de los requerimientos del software.

Mantiene los equipos de proyectos al día gracias a la creación, análisis y gestión de los requisitos de aplicaciones y casos de uso.

Sistema de publicación de aplicaciones PHP

Los sistemas de publicación de aplicaciones PHP son software de colaboración en actividades de desarrollo encaminadas a crear un sólido grado comercial y funcional, son plataformas en la que los individuos y las instituciones puedan construir sistemas fiables.

Gestores de base de datos.

Los sistemas gestores de base de datos son un conjunto de programas no visibles al usuario final que se encargan de la privacidad, la integridad, la seguridad de los datos y la interacción con el sistema operativo. Proporciona una interfaz entre los datos, los programas que los manejan y los usuarios finales.

4.2.4- Servicios ya implementados que se van a usar:

- DNS: Se utilizará el que tiene implementado la UCI (10.0.0.3 como principal y 10.0.0.4 como alternativo).
- Proxy: Se utilizará el que tiene implementado la UCI (10.0.0.1).

- Chat: Se utilizará el que tiene implementado la UCI (10.0.0.25).
- FTP: Se utilizará el que tiene implementado la UCI (10.0.0.22).
- Correo: Se utilizará el que tiene implementado la UCI, para el caso de nuestra facultad (10.0.0.35).
- Active Directory: Se utilizará el que tiene implementado la UCI.

4.2.5- Herramientas para el cumplimiento de los servicios

Anteriormente se muestran y explican los servicios instalados en los servidores, para la implementación de estos se seleccionaron un conjunto de herramientas que satisfacen las necesidades reales expuestas por el Proyecto CICPC, las mismas son:

Herramienta por servicio general:

- SubVersioN para el control de versiones.
- Trac para la gestión de proyectos.
- ProFTPd para el compartimiento de archivos.

SubVersioN.

Es un software libre bajo una licencia de tipo Apache/BSD y se le conoce también como **svn** por ser el nombre de la herramienta de línea de comandos. Una característica importante de SubVersioN es que todo el repositorio tiene un único número de versión que identifica un estado común de todos los archivos del repositorio en cierto punto del tiempo. Se integra con Apache HTTP Server [SubVersioN].

Trac.

Es un sistema de seguimiento de proyectos de desarrollo de software, utiliza un enfoque minimalista basado en la web de software de gestión de proyectos. La misión es ayudar a los desarrolladores a escribir grandes software mientras se mantienen al margen del camino. Ofrece una interfaz para el Subversion, integración con la Wiki y una excelente presentación de informes. Se integra con Apache HTTP Server [Trac].

ProFTPd.

Servidor FTP para la transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, se denomina como un “software servidor FTP altamente configurable y confiable con licencia GPL (licencia pública general de GNU)” [ProFTPd].

Herramienta por servicio específico:

- CruiseControl para el sistema de integración continua.
- Erwin Studio para el sistema de modelación de base de datos.

- Jakarta Tomcat para la publicación de aplicaciones JAVA.
- Paquete GFI LANGuard para la gestión de la configuración y la seguridad.
- Apache HTTP Server para la publicación de aplicaciones PHP.
- MySQL Server como gestor de base de datos para el Portal Web.
- Oracle 10g Release 2 como gestor de base de datos para la aplicación CICPC.
- Rational Requisite Pro 7.0 como herramienta para la gestión de requerimientos del software policial.

CruiseControl.

CruiseControl es una aplicación de código abierto basado en Java que permite la compilación automática de proyectos Java, utilizando Ant, Es una herramienta comúnmente utilizada en integración continua que cada cierto tiempo, o cuando hay cambios en el gestor de versiones (por ejemplo SubVersioN), hace una compilación y ejecuta pruebas, una vez acabadas las mismas, presenta el resultado final [CruiseControl].

Erwin Studio.

Es una herramienta de modelado para diseñar bases de datos. Ayuda a descubrir, documentar y reutilizar los datos activos. Con un soporte de ida y vuelta de bases de datos, permite analizar las fuentes de datos existentes, así como el diseño e implementación de bases de datos de alta calidad [Erwin].

Jakarta Tomcat.

Tomcat es un servidor web con soporte de servlets y JSPs. Incluye el compilador Jasper, que compila JSPs convirtiéndolas en servlets. El motor de servlets de Tomcat a menudo se presenta en combinación con el servidor web Apache [Tomcat].

Paquete GFI LANGuard.

GFI LANGuard escanea redes IP para detectar qué computadoras están funcionando. Luego intenta discernir la acogida del sistema operativo y qué aplicaciones se están ejecutando. Asimismo, trata de reunir el Windows Service Pack, parches de seguridad que falten, puntos de acceso inalámbrico, dispositivos USB, carpetas compartidas, puertos abiertos, servicios/aplicaciones activas en el ordenador, la clave de las entradas del registro, contraseñas débiles, usuarios y grupos, y más. Los resultados del análisis se guardan en un informe HTML, que puede ser personalizado. También incluye un gestor de parches que detecta e instala los parches que faltan. Para una mejor comprensión leer Capítulo 1 sobre los escáneres de red [GFI LANGuard].

MySQL Server.

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones, cumple con el estándar SQL, pero sin sacrificar velocidad, fiabilidad o usabilidad [MySQL].

Rational Requisite Pro 7.0.

Herramienta potente y fácil de utilizar para la gestión de requisitos y casos de uso, propicia una mejor comunicación, mejoras en el trabajo en equipo y reduce el riesgo de los proyectos.

Oracle 10g Release 2.

Oracle es un sistema de gestión de base de datos relacional. Hace posible el incremento de productividad y ahorro en costos para los administradores de bases de datos, reduce la complejidad. Ofrece diagnóstico y optimización del desempeño sin precedentes, además de excelente administración de los respaldos y recuperaciones [Oracle10g2].

4.2.6- Distribución de los servicios.

A partir de las características físicas expresadas anteriormente y atendiendo a los servicios a implementar para la puesta en marcha del Proyecto CICPC, se estructuran los servidores de la siguiente forma:

- Se reúnen los servicios que utilizan las mismas tecnologías.
- Se distribuyen los servicios en dependencia de las características físicas de los servidores.
- Se selecciona el sistema operativo que se va a instalar en los servidores.

Tabla 7: Distribución de servicios por servidores

Servidor	Servicios
Servidor 1	
	CruiseControl
	Erwin Studio
	Jakarta Tomcat
Servidor 2	
	GFI LANGuard
	Requisite Pro
Servidor 3	
	SVN
	Trac
	FTP
	Apache HTTP Server
	MySQL Server
Servidor 4	
	Oracle 10g Release 2
Integrity	
	Oracle 10g Release 2
	Jakarta Tomcat

Para la instalación y configuración del Jakarta Tomcat en HP-UX 11i v2, ver [Anexo 1].

Para la instalación y configuración del SubVersioN en Ubuntu 7.04, ver [Anexo 2].

Para la instalación y configuración del Trac en Ubuntu 7.04, ver [Anexo 3].

4.2.7- Selección de los sistemas operativos.

En el epígrafe anterior se presentan los servicios, tanto generales como específicos, distribuidos entre los cinco servidores con que cuenta el Proyecto CICPC. Verificando cada unos de estos servicios se detecta que algunas herramientas son nativas de la plataforma Windows, por lo que se hace necesaria la implantación de dicho sistema operativo en esos servidores.

Servidor 1

Se instalará el sistema operativo Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2. Su selección se debe a que solo se cuenta con la versión del Erwin Studio y el CruiseControl en la plataforma Windows.

Servidor 2.

Se instalará el sistema operativo Microsoft Windows Server 2003 Enterprise Edition, Service Pack 2. Su selección se debe a que se cuenta con la herramienta Requisite Pro, la cual solo soporta la plataforma Windows.

Servidor 3.

Se instalará el sistema operativo GNU/Linux, en su distribución UBUNTU 7.04. Las herramientas que se van a implementar para el cumplimiento de los servicios son

multiplataforma. La selección de UBUNTU 7.04 como sistema operativo se debe a la necesidad de simulación de una plataforma lo más cercana al UNIX que fue la seleccionada por el cliente para el Centro de Datos de los aplicativos; y como estrategia interna de la dirección de la Universidad y el proyecto.

Servidor 4.

Se instalará el sistema operativo GNU/Linux, en su distribución DEBIAN 3.1. El servicio que se va a implementar convierte al servidor en un servidor de base de datos, por lo que se requiere rapidez, confiabilidad y seguridad. La selección de DEBIAN 3.1 como sistema operativo se hizo por las mismas razones que el Servidor 3.

Servidor Integrity.

Se instalará el sistema operativo HP-UX 11i v2 (revisión empresarial más reciente para sistemas basados en la arquitectura Itanium con soluciones de software ampliadas y plataformas de hardware nuevas), además de que es el sistema operativo que se va a implementar en la solución del entorno final del cliente.

4.3- Criterios a tener en cuenta para la configuración.

En epígrafes anteriores se realizó el análisis y descripción de las características de los servidores del Proyecto CICPC, así como la distribución de los servicios generales y específicos que se van a implementar. A partir de esto se elaboraron un conjunto de criterios de configuración para proteger, mantener la integridad de la información almacenada y evitar el acceso de “login” por personal no autorizado, estos criterios de configuración están en correspondencia con el Plan de Seguridad informática expuesto en el Capítulo 2.

1. **De configuración de la red.**
    - La configuración TCP/IP de los servidores va a ser todo el tiempo estática, manteniendo el mismo IP desde la primera vez que prestó servicio. La misma será de la siguiente forma:
        - Subnet Mask:255.255.255.0
        - Default Gateway: 10.35.x.254 (x: depende del laboratorio donde esté ubicado)
        - Preferred DNS server: 10.0.0.3
        - Alternate DNS server: 10.0.0.4
    - El nombre de los servidores debe tener incluido el prefijo CICPC_SERVER para que exista distinción entre los demás equipos de cómputos del docente.

- Los servidores deben estar incluidos dentro del dominio UCI, efectuando esta tarea en conjunto con los administradores del Nodo Central, para el caso de los servidores montados en plataforma Linux.

2. **Del acceso a los servidores.**
   - Solo tendrá acceso de "login" a los servidores el siguiente personal:
     - Administradores de Sistema.
     - Jefe de Proyecto.
     - Jefe de Módulo que atiende directamente el servicio que presta el servidor.
   - Los servidores se manejan de forma remota, a no ser que ocurra alguna situación que disponga del manejo interactivo del mismo.
   - Se creará una cuenta local para cada persona con acceso al servidor, la misma se eliminará cuando esta persona ya no requiera de su uso.
3. **Del uso de los servicios.**
   - Solo pueden acceder a los servicios que brinda el servidor el personal que sea plantilla del Proyecto CICPC.
   - El uso del MySQL Server será exclusivamente para el desarrollo del Portal Web y solo tendrá permisos de modificar su configuración el Jefe de Subsistema del Grupo de Trabajo Portal Web.
   - El uso del Jakarta Tomcat en el servidor 1 y en el servidor Integrity será solo para los equipos de desarrollo y para el personal que se designe para las pruebas de calidad a la aplicación. Solo tendrán permisos de modificar su configuración los administradores de sistema del proyecto.
   - El uso del Erwin y del Oracle 10g Release 2 será solo para el personal del Grupo de Trabajo Base de Datos. solo tendrá permisos de modificar su configuración el Jefe de Subsistema del Grupo de Trabajo Base de Datos.
   - El uso del CruiseControl será solo para el despliegue de la aplicación en el Servidor Integrity, los responsables del mantenimiento serán los administradores de sistemas junto a Jefe de Subsistema del Grupo de Trabajo Arquitectos.
   - El uso del Requisite Pro será solo para los analistas del proyecto, el mantenimiento es responsabilidad de los administradores de sistema.
   - El acceso al FTP servidor será de solo lectura para el personal del Proyecto CICPC, excepto el personal que se autorice para subir información al servidor. Solo tendrán permisos de modificar su configuración los administradores de sistema del proyecto.

4. **De las configuraciones de los servicios.**
    - Los servicios deberán guardar en todo momento los logs para mantener las trazas de seguridad en caso de fallas.
    - El SubVersioN y el Trac estará configurado para la integración con un dominio LDAP (protocolo que permite el acceso a un servicio de directorio).
    - Al FTP se le configurará la velocidad de descarga para no sobrecargar el servidor en una de estas operaciones.
    - Al CruiseControl se le configurará la opción de que compile cada una hora mínimo.
    - Al Jakarta Tomcat se le incrementará el máximo de memoria reservada a 512 MB en el caso del servidor 1 y a 2 GB en el caso del servidor Integrity, con un mínimo de 256 MB y 756 MB respectivamente.
5. **De otras configuraciones.**
    - Para el caso de los servidores sobre plataforma Linux deberán tener deshabilitado el usuario root, a consecuencia todos los comandos se realizarán con el comando sudo.
    - Se habilitará el acceso remoto en cada servidor.
    - Se instalará y configurará en cada servidor dedicado el monitoreo de unos o varios de los cuatro subsistemas: CPU, disco duro, memoria e interfaz de red.

4.4- Políticas de respaldo y recuperación.

Siempre que se trabaja con información valiosa, es necesario contar con copias de seguridad. Las redes, lejos de ser una excepción, potencian esta necesidad puesto que guardan la información de todos los usuarios en un sólo lugar. Para evitar la pérdida de información se deben efectuar las copias de seguridad, también llamadas de respaldo y conocidas comúnmente como “backups”.

¿Qué es el respaldo y recuperación?

Es el proceso de restablecer las funcionalidades de una red informática después de una pérdida o error e la información lo más rápido posible y con la mayor similitud al estado antes de producirse el error.

El proceso de respaldo y recuperación se realiza a través de un Plan de Contingencia que se crea. El mismo tiene en cuenta las amenazas y vulnerabilidades a las que están expuestas las tecnologías informáticas, así como las acciones a realizar, los recursos a utilizar y el personal a emplear en caso de que se degraden o inutilicen los recursos informáticos del proyecto.

4.4.1- Reglas para el respaldo.

- Plan de respaldo con copias de seguridad rutinarias.
- Tener dos copias de seguridad, una en el proyecto y otra en exterior.
- Copia de seguridad del estado del sistema.
- Tener el disco de instalación localizable.

¿Qué es una copia de seguridad?

Es un proceso único que copia archivos y carpetas de una ubicación a otra. Hacerlo de forma regular en los discos duros del equipo cliente y del servidor previene la pérdida de datos provocada por errores de la unidad de disco, interrupciones del suministro eléctrico, infecciones por virus y otros incidentes similares, la misma garantiza:

- La continuidad del proyecto.
- La recuperación de datos.
- Contención de problemas derivados por errores físicos o lógicos.

La copia de seguridad presenta los siguientes problemas:

- Garantizar que cuando se trate de copiar los ficheros estos no estén en uso. De otra forma podrían estar bloqueados y no copiarse correctamente.
- Disponer del suficiente espacio externo siempre.
- Conocer donde se encuentra la información esencial.
- Mantener y actualizar las fuentes de información para evitar pérdidas.
- Proporcionar métodos que no sean intrusivos con la actividad del proyecto.

Conociendo lo anteriormente expuesto se presenta el proceso que va a llevar a cabo el Proyecto CICPC para no afectar en ningún momento la continuidad del proyecto.

4.4.3- Proceso para el respaldo y recuperación de la información.

Para el proceso de respaldo y recuperación de la información se definir una serie de pasos o procedimientos para verificar las principales actividades.

4.4.3.1- ¿Qué es lo importante a respaldar?

Al no contar con servidores de respaldo donde se pueda almacenar toda la información y configuración de los servidores del Proyecto CICPC, y al no tener espacio suficiente, se prioriza lo siguiente:

- **Servidor 1:**
    - Ficheros de configuración de los servicios.
    - Datos de relevancia del Erwin Studio.

- **Servidor 2:**
  - Datos de relevancia de los procesos de auditoría realizados.
- **Servidor 3:**
  - Ficheros de configuración de los servicios.
  - La información guardada en el SubVersioN.
  - Datos relevantes del Trac.
  - La información relevante del proyecto presente en el FTP.
  - La información guardada en la carpeta www del Apache HTTP Server.
  - Las bases de datos del MySQL Server.
- **Servidor 4:**
  - Ficheros de configuración y las bases de datos del Oracle 10g Release 2.
- **Servidor 5:**
  - Instalación inicial del sistema operativo.
  - Ficheros de configuración de los servicios.
  - Las bases de datos del Oracle 10g Release 2.

4.4.3.2- Tipos de respaldo a realizar.

Podemos distinguir la copia de seguridad según el tipo de respaldo que realiza. Es decir, si los datos son difícilmente recuperables o no. En general todos los datos que afectan tanto a la continuidad del proyecto como a la actividad del mismo, son datos que difícilmente se pueden restablecer después de la pérdida de unos de ellos, por esto disponen de una prioridad mayor en cuanto a su salvaguarda. Los datos que afectan al sistema operativo, generalmente se pueden recuperar.

Las diferentes copias de seguridad que existen son:

Tabla 8: Tipos de copia de seguridad.

Tipo	Acción realizada	Borra el atributo del archivo
Normal	Archivos y carpetas seleccionados.	Si
De copia	Archivos y carpetas seleccionados.	No
Diferencial	Archivos y carpetas seleccionados que hayan cambiado desde la última copia de seguridad normal o incremental.	No
Incremental	Archivos y carpetas seleccionados que hayan cambiado desde la última copia de seguridad.	Si
Diaria	Archivos y carpetas que hayan cambiado a lo largo del día.	No

A partir de los problemas existentes se decide utilizar los tipos de respaldo normal e incremental. Se escoge la copia de seguridad incremental ya que en el proceso se hace una

copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad realizada, esto ahorra en espacio y hace que sea más rápido el respaldo.

4.4.3.3- Cantidad de respaldos a realizar.

La programación de los respaldos que se van a realizar a lo largo de la semana son:

Tabla 9: Programación de los respaldos.

Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
Normal	Incremental	Incremental	Incremental	Incremental	Incremental	Incremental

Cuando pase un ciclo semanal se eliminará las copias de seguridad de la semana anterior para así poder almacenar las correspondientes a esta semana.

4.4.3.4- Horario.

El respaldo se debe realizar en un momento del día donde no haya usuarios conectados realizando cambios en la información que se va a respaldar. Se propone realizarla de la siguiente forma:

Tabla 10: Horario de los respaldos.

Respaldo	Hora inicial.	Frecuencia
Normal.	03:00 AM.	Semanal.
Incremental.	04:00 AM.	Diaria.

4.4.3.5- Localización de los respaldos.

La localización es el lugar donde se van a guardar las copias de seguridad. Por el momento se guardaran en el Servidor 2, disponiendo para esto con una capacidad de 100GB.

4.4.3.6- Recuperación ante fallos.

En el momento en que ocurra un fallo que puede ser: perdida de la información contenida en los servidores, destrucción o modificación del sistema operativo o servicios; se procede a la recuperación del estado del servidor de la siguiente forma:

1. Restauración de la copia de seguridad normal de la semana.
2. Restauración de la copia incremental de los días anteriores a la rotura.

Este es un proceso un poco lento porque hay que realizar varias restauraciones, pero nos ayuda en minimizar la capacidad de almacenamiento.

4.5- Conclusiones.

En este capítulo se definieron las características de los servidores con que cuenta el Proyecto CICPC, se exponen los criterios a tener en cuenta para la configuración, tanto de los servicios, como de los servidores. Se muestran las políticas de respaldos y recuperación creadas para la protección de la información en caso de fallas.

CAPÍTULO 5

RESULTADOS OBTENIDOS

5.1- Introducción.

En este capítulo se expondrán los beneficios que aportó esta investigación para el Proyecto CICPC, a partir de la implantación de las políticas de seguridad, los procedimientos y las creaciones de los ambientes de desarrollo para los equipos de trabajo; además de presentar las principales violaciones de los artículos expresados en el Plan de Seguridad que son detectadas mediante las auditorías y las sanciones aplicadas en cada caso.

5.2-Beneficios de la creación del Entorno controlado de Desarrollo.

La creación y aplicación del Entorno Controlado de Desarrollo para los Grupos de Trabajo del Proyecto CICPC ha minimizado el tiempo de respuesta en los procedimientos que se realizan comúnmente cuando ocurre una rotura, ya sea de hardware o software, o cuando se requiere un mantenimiento a la computadora para un mejor rendimiento.

La creación de los Grupos de Trabajo ha aportado lo siguiente para el desarrollo del proyecto:

- Especialización de las herramientas por Grupo de Trabajo, evitando así una sobrecarga del rendimiento de la computadora.
- División de las responsabilidades por Grupo de Trabajo.
- Optimizar el rendimiento de las computadoras.
- Minimizar el tiempo que se demora en instalar y configurar el sistema operativo y las herramientas que se utilizan.
- Llevar un control de versiones de las herramientas que se utilizan.
- Cumplir con el Plan de Seguridad Informática, a partir de las políticas de seguridad configuradas.
- Inclusión del antivirus activado, esto posibilita no contaminarse de virus la primera vez que se conecten a la red.
- Mantenimiento controlado de las herramientas que se utilizan.
- La misma configuración de las herramientas en todas las computadoras.

5.2.1- Tiempo ahorrado.

En este epígrafe se hará un análisis del tiempo ahorrado después de implantado el Entorno Controlado de Desarrollo, usando tiempos aproximados de cuanto demora instalar y configurar una por una, cada computadora del Proyecto CICPC.

Variables:

- TSO: tiempo que se demora instalando el sistema operativo.
- THBASE: tiempo que se demora instalando y configurando las herramientas base.
- THGT: tiempo que se demora instalando y configurando las herramientas de los Grupos de Trabajo.
- PC: Cantidad de computadoras.
- TP: tiempo de preparación de las computadoras.
- TIMG: tiempo que demora montando la imagen.
- TCONF: tiempo de las configuraciones posteriores.
- SA: cantidad de administradores de sistemas.
- TT1: tiempo total que demora sin imagen.
- TT2: tiempo total con imagen.
- TH: tiempo ahorrado.

Tabla 11: Tiempo aproximado de las variables.

Variables.	Tiempo aproximado.
TSO	30 min
THBASE	60 min
THGT	30 min
PC	60
TP	20 min
TIMG	30 min
TCONF	10 min
SA	2

En las tablas que se muestran a continuación se identifican los tiempos que consumen cada uno de los procedimientos, los valores son aproximados ya que los mismos varían en dependencia de las características de la computadora.

Instalando y configurando una computadora.

Tabla 12: Tiempo aproximado de instalación.

Variables.	Ecuación.	Valor aproximado
TT1	$(TSO + THBASE + THGT)$	120 min
TT2	$TIMG + TCONF$	40 min
TH	$\boldsymbol{TT1 - TT2}$	**80 min**

Como resultado se obtiene un ahorro de 80 minutos montando una imagen que instalando y configurando Windows manualmente. En el tiempo que se monta la imagen el responsable de la computadora puede aprovecharlo en cualquier otra computadora que esté desocupada, y así no se atrasa en su labor.

Instalando y configurando todas las computadoras del proyecto.

Tabla 13: Tiempo aproximado de instalaciones.

Variables.	Ecuación.	Valor aproximado.
TT1	$(TSO + THBASE + THGT) \times PC \div SA$	3600 min (60 horas)
TT2	$TP + TIMG + (TCONF \times PC) \div SA$SA	350 min (5.8 horas)
TH	$\boldsymbol{TT1 - TT2}$	**3250 min (54.2 horas)**

Como resultado se obtiene un ahorro de 3250 minutos montando todas las imágenes al mismo tiempo. El tiempo que se ahorra con este procedimiento es tiempo que el proyecto aprovecha para el desarrollo de los aplicativos.

5.2.2- Datos recogidos con el transcurso del tiempo.

Actualmente están implementadas y configuradas todas las imágenes propuestas en el Capítulo 3, las mismas se pusieron a prueba en el inicio del proyecto para verificar el comportamiento de las mismas. En un principio el desarrollo fue un poco inestable ya que la mayoría de las veces ocurrían fallas en el funcionamiento del sistema operativo o se cambiaba la configuración de una de las herramientas. Con el transcurso del proceso de desarrollo del Proyecto CICPC se estabilizó el Ambiente de Desarrollo dando como resultado que todos los Grupos de Trabajo desarrollarán sin interrupciones los diferentes aplicativos.

A continuación se mostrará un histórico de los procesos realizados desde el momento de la implantación con una explicación del por qué fueron necesarios, esto puede dar una medida del nivel de aplicabilidad que tuvieron los procesos diseñados:

Tabla 14: Datos recogidos.

No.	Proceso.	Cant.	Descripción.
1.	Montaje general de imágenes.	3	Las imágenes en forma general se efectuaron la primera vez que se configuró el Entorno Controlado de Desarrollo cuando se realizó el primer cambio de Laboratorio de Proyecto; y las demás en dependencia de las actualizaciones de las herramientas que se hicieron. Para este caso se aplicó el procedimiento: “montaje de las imágenes”.

2.	Montaje aislado de imágenes.	± 60	Estas imágenes aisladas se deben a un fallo del sistema operativo, lo que provoca que la computadora no inicie. El procedimiento correspondiente para este caso es: “mantenimiento de software”.
3.	Mal funcionamiento de software.	± 100	Estos mal funcionamientos de debe a la pérdida de la configuración de la herramienta que presenta problemas, provocando que no funcione correctamente. Para este caso se aplicó el procedimiento: “mantenimiento de software”.
4.	Actualizaciones de software.	2	Este proceso se realizó en 2 ocasiones, ya que, la primera fue para corregir todos los errores y defectos que tenía el primer Entorno Controlado de Desarrollo y la segunda vez para actualizar las versiones de todas las herramientas. Para este caso se aplicó el procedimiento: “actualización del software”.
5.	Actualización general de hardware.	2	- **Laboratorio 208.** Las actualizaciones en cuestión fueron la adición de una memoria RAM de 512MB para incrementar el rendimiento de la computadora, ya que la plataforma JAVA consumía muchos recursos haciendo el trabajo demasiado lento. Para este caso se aplicó el procedimiento: “actualización del hardware de la computadora”. - **Laboratorio 207 y 208.** Las actualizaciones en cuestión fueron el cambio de la memoria de 256MB por una de 1GB para el caso del laboratorio 207 que no había sido actualizado y el cambio de las memorias de 512MB y 256MB por una de 1GB para el caso del laboratorio 208. Para este caso se aplicó el procedimiento: “actualización del hardware de la computadora”.

6.	Actualización aislada de hardware.	2	Las actualizaciones aisladas que se han realizado en los laboratorios del Proyecto CICPC fueron el cambio de los lectores de DVD por quemadores de CD en los servidores 3 y 4, además de la adición de un disco duro SATA de 80GB para los mismos servidores y el incremento de la memoria RAM. Para este caso se aplicó el procedimiento: "actualización del hardware de la computadora".
7.	Mantenimiento general de hardware.	1	El mantenimiento de hardware de todas las computadoras de los laboratorios se debió a la programación que tiene COPEXTEL para limpiar cada componente interno de las mismas. El procedimiento correspondiente para este caso es: "mantenimiento de hardware".
8.	Mantenimiento aislado de hardware.	± 50	El mantenimiento aislado a las computadoras se debe a alguna rotura de alguno de los componentes internos, esta rotura puede ser que se arregle en el momento o esperar a que le cambie la pieza con problemas. El procedimiento correspondiente para este caso es: "mantenimiento de hardware".
9.	Actualizar políticas de seguridad.	± 40	El cambio de las políticas de seguridad se debió en su momento al ingreso o egreso de estudiantes al Proyecto CICPC, esto trae como consecuencia la actualización de los grupos de usuarios de cada computadora del proyecto. El procedimiento correspondiente para este caso es: "actualizar políticas de seguridad".
10.	Auditorías realizadas.	8.	Los procesos de auditoría realizados ayudaron a detectar violaciones de las políticas de seguridad impuestas en las imágenes, además ayudan a la detección de intrusos. El procedimiento correspondiente para este caso es: "proceso de auditoría".

Si se efectúan los cálculos anteriores a los datos recogidos con el transcurso del tiempo se percibe que el tiempo ahorrado para la labor de instalación y configuración de las computadoras se reduce grandemente gracias al Entorno Controlado de Desarrollo y los procedimientos llevados a cabo por los administradores de sistemas para resolver los problemas presentes en los laboratorios.

Computadoras aisladas.

Tabla 15: Tiempo aproximado de las computadoras aisladas.

Variables.	Ecuación.	Valor aproximado
TT1	$(TSO + THBASE + THGT)$ * 60	7200 min (300 horas)
TT2	$(TIMG + TCONF)$ * 60	2400 min (100 horas)
TH	$\boldsymbol{TT1 - TT2}$	**4800 min (200 horas)**

Montaje en general.

Tabla 16: Tiempo aproximado de las computadoras aisladas.

Variables.	Ecuación.	Valor aproximado.
TT1	$((TSO + THBASE + THGT) \times PC \div SA)$ * 3	10800 min (450 horas)
TT2	$(TP + TIMG + (TCONF \times PC) \div$ SA) * 3	350 min (43.75 horas)
TH	$\boldsymbol{TT1 - TT2}$	**10450 min (435.5 horas)**

5.3- Servidores.

Actualmente en el Proyecto CICPC se encuentran funcionando los 5 servidores que brindan los diferentes servicios para el proceso de desarrollo. Los mismos han desempeñados disímiles tareas en dependencia de sus funcionalidades y su capacidad física. A continuación se presenta un cuadro resumen donde se expone lo anteriormente dicho:

Tabla 17: Tareas por servidores.

Servidor	Tarea que ha desempeñado.	Descripción.
Servidor 1	Montar imágenes.	Esta tarea estuvo implementada para el montaje de las imágenes del laboratorio 208, en él se guardaba el Entorno Controlado de Desarrollo del Proyecto CICPC.
	Contenedor de servlets.	El contenedor de servlets es la implementación de Apache Tomcat, esta tarea estuvo vigente para las pruebas de calidad interna. Con la llegada del

		servidor Integrity al proyecto su uso fue para el WEB SERVICES y para el mock de un cliente de la aplicación.
	Modelación de la base de datos.	Esta tarea se mantiene en vigencia, el uso de la misma es para el Grupo de Trabajo Base de Datos.
	Integración continua.	Esta tarea es la que mantiene actualmente para la compilación de la aplicación.
Servidor 2	Montar imágenes.	Esta tarea se mantiene en vigencia para el montaje de las imágenes de los laboratorios del proyecto. Aquí está guardado el Entorno Controlado de Desarrollo.
	Gestión de la red	La gestión de la red no es más que el monitoreo en tiempo real con el Paquete GFI LANGuard. Esta tarea se mantiene actualmente para el proceso de auditoría interna a las computadoras del Proyecto CICPC.
	Contenedor de los respaldos.	En este servidor es donde se alojan los respaldos que se le hacen a los servidores.
Servidor 3	Control de versiones.	Es una de las tareas de mayor peso en el proyecto ya que gracias a esto se mantienen los cambios realizados para todos los Grupos de Trabajo.
	Compartimiento de archivos.	El compartimiento de archivos del proyecto se realiza a través del FTP, esta tarea se mantiene en vigencia.
	Gestión de proyectos.	Esta tarea actualmente está en uso.
	Contenedor WEB.	Tarea que despeña junto al MySQL SERVER para el montaje del portal del Proyecto CICPC, actualmente sigue

		prestando este servicio.
Servidor 4	Gestor de base de datos.	Actualmente esta tarea esta en ejecución en el proyecto, la base de datos que aquí se aloja es la oficial.
Integrity	Contenedor de servlets	Esta tarea aún está vigente, su uso es para las pruebas de calidad UCI e interna. También se utiliza para las mostrar los avances de la aplicación.
	Gestor de base de datos	Tarea que está en uso, la base de datos que aquí se aloja es la que usan los programadores para las pruebas a la aplicación.

5.4- Proceso de auditoría para las computadoras del Proyecto CICPC.

Los procesos de auditoría del Proyecto CICPC ayudan a la gestión de la configuración y la seguridad del Entorno Controlado de Desarrollo, detecta las amenazas presentes en la red por ataques de virus troyanos, informan sobre las vulnerabilidades existentes en las computadoras y brinda reportes completos del estado actual del proyecto en concordancia con la seguridad.

La herramienta seleccionada para ejecutar esta actividad es el Paquete de GFI LANGuard, la misma cuenta con varios módulos o programas que cada uno tiene sus funcionalidades específicas, los siguiente módulos son los que van a ser usados en el proyecto.

- GFI LANGuard N.S.S (Network Security Scanner).
- GFI LANGuard S.E.L.M (Security Event Log Monitor).

5.4.1- GFI LANGuard N.S.S.

El presente módulo se encarga del escaneo en tiempo real a partir del rango de IP que se le defina, la misma tiene los siguientes filtros:

- Reporte completo.
- Vulnerabilidades altas.
- Vulnerabilidades Medias.
- Todas las vulnerabilidades.
- Puertos abiertos.

- Carpetas compartidas.
- Políticas de audición.
- Políticas de contraseñas.
- Detección de contraseñas débiles.
- Usuarios y grupos de usuarios.

En las auditorías que se han implementados se han encontrado disímiles violaciones contra el Plan de Seguridad Informática del proyecto, a continuación se exponen dichas violaciones con su artículo correspondiente.

Tabla 18: Violaciones detectadas.

No.	Violación detectada	Artículo	Medida disciplinaria.
1	Obtención de la dirección IP por DHCP.	16	Falta Leve.
2	Computadoras sin el prefijo CICPC en el nombre.	17	Falta Leve.
3	Computadoras fuera del dominio UCI.	13	Falta Grave.
4	Escritorio remoto activado en la computadora.	24	Falta Grave
5	Carpetas compartidas en las computadoras.	22	Falta Grave
6	Contraseñas del BIOS cambiadas.	26	Falta Grave
7	Transformación del Entorno Controlado de Desarrollo.	29, 30, 32	Se convierte en Falta Grave.
8	Modificación del Grupo de Usuarios CICPC.	29, 30	Se convierte en Falta Grave.
9	Cuentas locales con permisos administrativos no autorizadas.	29, 32	Se convierte en Falta Grave
10	Cuentas locales administrador e invitados habilitadas.	29, 33	Se convierte en Falta Grave
11	Detección de cuentas con permisos administrativos ajenos al proyecto.	12, 20, 29	Falta muy Grave.
12	Detección de cuentas con permisos administrativos en computadoras no autorizadas.	10, 29	Falta Grave.
13	Detección de usuarios ajenos al proyecto conectados a carpetas compartidas en las computadoras.	22, 24	Se convierte en Falta muy Grave.
14	Modificación de la cuenta sysadmin.	29, 30, 34	Falta Grave.
15	Puertos no autorizados abiertos en las computadoras.	30	Falta Leve.

La tabla anterior muestra las principales violaciones detectadas durante las auditorías que se hicieron a lo largo del transcurso del Proyecto CICPC. Por política del Proyecto si una

persona ya tiene una medida leve y vuele a incidir en otra medida leve, esta se convierte en grave y así sucesivamente hasta que no cumpla el tiempo de la sanción.

Hay que destacar que en una de las auditorías realizada se detectó un “Backdoors (3127 mydoom)” que usualmente es utilizado por troyanos. Mydoom según los especialista es la más rápida propagación de virus de correo electrónico registrada todavía, el mismo abre el puerto 3127 que permite a un intruso ejecutar códigos de forma remotas. Para contrarrestarlo se debe bloquear el puerto 3127 en el “cortafuegos” de la computadora.

También se detectó una vulnerabilidad de tipo “rpc.ypasswdd” donde un usuario malicioso pudo ser capaz de explotar esta vulnerabilidad para sobrescribir los lugares sensibles en la memoria, posibilitando que pudiera ejecutar código arbitrario con privilegios administrativos, esta intrusión fue detectada a tiempo gracias a la auditoría.

5.4.2- GFI LANGuard S.E.L.M.

El módulo GFI LANGuard S.E.L.M se encarga de monitorear los log que generan los eventos de seguridad de la computadora escaneada. El mismo genera reportes para mantener al administrador de sistema de las acciones llevadas por los usuarios. A continuación se presentan algunos de estos reportes, destacar que esto se hace en un período de tiempo comprendido: hoy, ayer, últimos siete días, este mes.

Porcentaje de reporte de usuarios.

- Porcentaje de usuarios que no pudieron conectarse.
- Usuarios que se conectaron satisfactoriamente.
- Usuarios que fallaron la conexión porque el usuario y la contraseña era incorrecta.

Gracias a este reporte el administrador de sistema puede hace un seguimiento del porciento de conexión de un usuario a una computadora, y así detectar posibles intrusos.

Reporte de evento de usuarios.

- Primer usuario conectado a la computadora.
- Actividades importantes de las cuentas de usuarios.

Reporte de eventos en cada computadora.

- Login satisfactorio.
- Acciones de los usuarios.
- Posible manipulación de los log de auditoría de la computadora.

Los reportes que genera este módulo son precisos y correctos, en algunos casos ayudan a detectar a tiempo cualquier cambio en las política de seguridad y da la posibilidad de ver quien, donde y cuando fue que se hizo.

En la siguiente tabla se muestran algunos ejemplos de eventos detectados no acordes al Plan de Seguridad Informática.

Tabla 19: Eventos detectados.

No.	Categoría	Fuente	Tipo	Fecha	Descripción.
1	Administración de cuentas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha añadido una cuenta al grupo local Administradores.
2	Administración de cuentas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha añadido una cuenta al grupo local SQLServer2005.
3	Administración de cuentas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha eliminado un usuario perteneciente al Grupo de Administradores.
4	Administración de cuentas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha hecho un cambio en la cuenta sysadmin en la computadora X.
5	Administración de cuentas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha eliminado un usuario del Grupo de Usuarios CICPC.
6	Cambios de políticas.	Seguridad	Éxito	2/06/2008	El usuario X del dominio X ha cambiado las políticas de auditoría en la computadora X.

En estos eventos se observan todas las acciones llevadas a cabo por los usuarios o por la computadora, para así poder detectar cualquier cambio que ocurra que atente contra las políticas de seguridad o viole cualquier artículo descrito en el Plan de Seguridad Informática. Monitorear estos eventos es lo que verdaderamente debe hacer un administrador de sistema para mantener tener una gestión de la red segura y confiable.

5.5- Conclusiones.

En este capítulo se mostraron ejemplos de los procesos de auditoría realizados a las computadoras del proyecto CICPC y las medidas aplicadas en cada caso según lo que dicta el Plan de Seguridad Informática. Se realizó un análisis del tiempo ahorrado gracias a la implementación del Entorno Controlado de Desarrollo, además de un muestreo de los principales datos recogidos a lo largo del tiempo.

CONCLUSIONES

El proceso de creación del presente trabajo ha atravesado diferentes etapas dando cumplimiento a los objetivos del mismo. Inicialmente se elaboró y se dio a conocer el Plan de Seguridad Informática a los miembros del proyecto para que tuvieran conocimiento del mismo. Posteriormente se trazaron las líneas base para la configuración de los servidores y del Entorno Controlado de Desarrollo, para luego implantarlo en las computadoras del Proyecto CICPC.

Una vez implementado el Entorno Controlado de Desarrollo se pasó a la selección de la herramienta para la gestión de la configuración y la seguridad de la red de los laboratorios.

Como resultado de dicha herramienta se pudo constatar cuales eran las principales amenazas a que se sometían diariamente los activos del proyecto, a través de esto se fueron incrementando las políticas de seguridad para así llegar a una configuración estable que minimizara los daños.

Esta propuesta contribuye al fortalecimiento del proceso de enseñanza - aprendizaje de los futuros administradores de sistema del Proyecto CICPC, quedando cumplidos los objetivos de manera satisfactoria.

RECOMENDACIONES

Una de las causas que hacen más riesgosa la seguridad del Proyecto CICPC son las laptops, ya que por la movilidad de estos se hace casi imposible controlar la información almacenada en su disco duro con el diseño actual de configuraciones del Plan de Seguridad Informática.

Por lo que se recomienda que se obtengan los permisos pertinentes en los locales de redes y seguridad informática de la UCI para establecer en el Servidor 2 un servicio DHCP con el cual se otorgarían las direcciones dinámicas a todas las computadoras que se encuentren en los dominios de nuestro proyecto. De esta manera se recogen las características de cada computadora, incluyendo las laptops, a los cuales se le daría una dirección IP según su “MAC Address (Media Access Control)”, de esta manera quedaría registrado en el servidor la laptop que se conecte a la red de los laboratorios del Proyecto CICPC y se asegura que las únicas autorizadas a trabajar con la información sean estas.

Velar por el cumplimiento del Plan de Seguridad Informática y efectuar las medidas disciplinarias siempre que sean necesarias.

Perfeccionar el Plan de Seguridad Informática y adaptar el proyecto a las especificaciones del mismo y no condicionar el Plan a las características actuales del proyecto, ya que de esta forma se evidencian debilidades importantes en la seguridad.

REFERENCIA BIBLIOGRÁFICA

[NC-17799] Oficina Nacional de Normalización, Norma Cubana NC-ISO-IEC 17799, Publicada en 2005, Ciudad de la Habana.

[NC-27001] Oficina Nacional de Normalización, Norma Cubana NC-ISO-IEC 27001, Publicada en 2005, Ciudad de la Habana.

[IntMont] Redes Informáticas. [Consultado en: Febrero, 2008]. Disponible en: http://www.networks.com

[MontRed] Monitoreo y evaluación. [Consultado en: Febrero, 2008]. Disponible en: http://www.cinterfor.org.uy/public/spanish/region/ampro/cinterfor/temas/gender/em_ca_eg/m_eva.htm

[SegDatos] Normas de Seguridad de Datos. [Consultado en: Febrero, 2008]. Disponible en: https://www.pcisecuritystandards.org/pdfs/spanish_pci_security_scanning_procedures_v1-1.pdf

[Nessus] NESSUS, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.nessus.org/nessus/

[GFI LANGUARD] GFI LANGUARD, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.gfi.com/lannetscan

[CoreImpact] CORE IMPACT, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=32

[InternetScanner] INTERNET SCANNER, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.iss.net./products/Internet_Scanner/product_main_page.html

[SARA] SARA, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www-arc.com/sara/

[QualysGuard] QUALYSGUARD, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: QualysGuard: http://www.qualys.com/solutions/vulnerability_management

[SAINT] SAINT, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.secureroot.com/security/tools/9665296466.html

[MBSA] MICROSOFT BASELINE SECURITY ANALYZER, Sistema de monitoreo de red. [Consultado en: Febrero, 2008]. Disponible en: http://www.microsoft.com/technet/security/tools/mbsahome.mspx

BIBLIOGRAFÍA

[Office] MICROSOFT OFFICE, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.microsoft.com/spain/Office/prodinfo.mspx

[TortoiseSVN] Stefan Küng, Lübbe Onken y Simon Large. *TortoiseSVN, Un cliente de Subversion para Windows. Polonia: 2006*

[JVM] JAVA VIRTUAL MACHINE, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.java.com/es/download/manual.jsp

[AcrobatReader] ADOBE ACROBAT READER, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.uned.es/csi/sai/software/acrobatReader/index.htm

[AD-Aware] AD-AWARE, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.lavasoftusa.com/

[NortonGhost] NORTON GHOST, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.symantec.com/es/es/business/products/newfeatures.jsp?pcid=2247&pvid=865_1

[Kaspersky] KASPERSKY, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.segurmatica.co.cu/gruporedes/gr1.jsp

[Mozilla] MOZILLA, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.mozilla-europe.org/es/products/firefox/

[Paradigm] VISUAL PARADIGM, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.freedownloadmanager.org/es/downloads/Paradigma_Visual_para_UML_(M%C3%8D)_14720_p/

[Tomcat] JAKARTA TOMCAT, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://tomcat.apache.org/

[Eclipse] ECLIPSE, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.eclipse.org/

[Exadel] EXADEL STUDIO, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.exadel.com/web/portal/products/ExadelStudioPro

[RedHat] RED HAT DEVELOPER STUDIO RELEASE CANDIDATE 1, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.linuxparatodos.net/portal/article.php?story=20070815100607134

BIBLIOGRAFÍA.

[Postgre] POSTGRESQL, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.sobl.org/traducciones/practical-postgres/node19.html

[MySQL] MYSQL, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.mysql.com/

[Erwin] ERWIN STUDIO, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.embarcadero.com/

[InstClient] INSTANT CLIENT, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.oracle.com/technology/software/tech/oci/instantclient/index.html

[PLSQL] PLSQL DEVELOPER, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://descargas.vnunet.es/descargas/bases+de+datos/pl+sql+developer/_33973.html

[Aptana] APTANA, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.genbeta.com/2006/07/26-aptana-ide-para-aplicaciones-ajax

[Apache] APACHE HTTP SERVER, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://httpd.apache.org/

[PHP] HYPERTEXT PREPROCESSOR, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.php.net/

[EMS] ENTERPRISE MANAGER SYSTEM, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.programacionphp.net/recursos-programas/programas-de-bases-de-datos/EMS-MySQL-Manager-Professional-3.2_9.html

[NuSphere] NUSPHERE PHPED, Herramientas del Entorno. [Consultado en: abril, 2008]. Disponible en: http://www.programacionphp.net/recursos-programas/programas-de-editores-de-php/NuSphere-PHPEd-3.3.3_12.html

[SVN] CONTROL DE VERSIONES, Servicios generales. [Consultado en: abril, 2008]. Disponible en: http://svnbook.red-bean.com/index.es.html

[IntCont] INTEGRACIÓN CONTINUA, Servicios generales. [Consultado en: abril, 2008]. Disponible en: http://cruisecontrol.sourceforge.net/

[ModDB] MODELACIÓN DE BASE DE DATOS, Servicios generales. [Consultado en: abril, 2008]. Disponible en: http://elies.rediris.es/elies9/4-2.htm

[SubVersioN] SUBVERSION, Herramientas por servicios. [Consultado en: abril, 2008]. Disponible en: http://subversion.tigris.org/

BIBLIOGRAFÍA.

[Trac] TRAC, Herramientas por servicios. [Consultado en: abril, 2008]. Disponible en: http://trac.edgewall.org/

[ProFTPd] PROFTPD, Herramientas por servicios. [Consultado en: abril, 2008]. Disponible en: http://www.proftpd.org/

[CruiseControl] CRUISE CONTROL, Herramientas por servicios. [Consultado en: abril, 2008]. Disponible en: http://cruisecontrol.sourceforge.net/

[Oracle10g2] ORACLE 10G RELEASE 2, Herramientas por servicios. [Consultado en: abril, 2008]. Disponible en: http://www.oracle.com/

GLOSARIO DE TÉRMINOS

Hardware: parte física de un computador y más ampliamente de cualquier dispositivo electrónico.

Software: equipamiento lógico o soporte lógico de un computador digital, comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema.

Enrutadores (routers): dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red).

Activo Informático: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

Amenaza: es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales de sus activos.

Scanner: dispositivo de entrada que permite digitalizar imágenes y documentos.

Hub: dispositivo que permite centralizar el cableado de una red y poder ampliarla.

Switch: dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Auditoría: examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.

Aplicativos: Aplicaciones realizadas dentro del Proyecto CICPC.

Cron: Fichero para la programación de tareas en un tiempo especificado.

API: conjunto de funciones y procedimientos que ofrece cierta biblioteca para se utilizada por otro software como una capa de abstracción.

ANEXOS

[Anexo 1]. Instalación y configuración del Jakarta Tomcat en HP-UX 11i v2.

Para el despliegue de la aplicación hay que instalar estos programas:

1. Apache Tomcat 5.5.20
2. OpenSSL
3. Java 1.5
4. Jre 1.5

Pasos para la instalación y configuración del Tomcat 5.5.20.

1. Poner el disco de instaladores en la torre de DVD del servidor.
2. Logearse como root para tener los permisos pertinentes.
3. Abrir una consola y en el "prompt" ejecutar el siguiente comando "swinstall" y dar "Return" al cuadro de diálogo que aparece.
4. En el siguiente cuadro de diálogo se debe elegir la fuente de donde se quiere instalar el paquete de software
    a. En la opción "Source Depot Type" tienen tres opciones
        i. "Local CDROM" permite instalar desde la torre de CDROM directamente.
        ii. "Local Directory" permite instalar desde el disco local. En la opción "Source Depot Path" se especifica el "almacén de software" donde se encuentra el instalador.
        iii. "Local Tape" permite instalar desde una cinta
        iv. "Network Directory/CDROM" permite instalar un software que se encuentra en otro servidor. Para esto en la opción "Source Host Name" se especifica el nombre del servidor y en la opción "Source Depot Path" se especifica el "almacén de software" donde se encuentra el instalador necesitado.
    b. Después de haber seleccionado desde donde se va a instalar procede a dar "Ok".
5. En el siguiente cuadro de diálogo aparecen todos los software que se encuentran en dentro de la fuente que se escogieron anteriormente.
    a. Aquí se selecciona el "Apache Tomcat 5.5.20" y se procede a marcarlo para la instalación. Para marcar un software debemos dar "barra espaciadora" para seleccionarlo y luego presionar la tecla "m" para marcarlo.
    b. Después de haber marcado el software vamos al menú "Actions" y se selecciona la opción "Install", donde se abre el cuadro de diálogo "Install Analysis".

c. Se espera a que el análisis se complete satisfactoriamente para proseguir con la instalación. Cuando termine el análisis se selecciona la opción “Ok”, desde donde se procede a la fase final de la instalación.

6. En el último paso para la instalación se verifica que se haya instalado sin errores, para esto se va al prompt y se ejecuta el siguiente comando:

   $ vi /var/adm/sw/swagent.log

   Este es el fichero de “logs” del agente de instalación, aquí se ven todo los problemas en la instalación del programa, solo se debe buscar la fecha y la hora en que comenzó la instalación.

Una vez instalado el Apache Tomcat 5.5.20 se pasa a la instalación de la máquina virtual de java y al OpenSSL, procediendo de la misma forma. Los instaladores que se necesitan son Java1.5, Jre1.5 y OpenSSL.

Antes de pasar a configurar el Apache Tomcat 5.5.20 se muestran los principales directorios en que se trabaja:

1. El directorio donde se instala es /opt/hpws/tomcat
2. El servicio para reiniciar y parar el servidor se encuentra en /sbin/init.d/
3. El binario /etc/rc.config.d/hpws_tomcatconf es donde se especifica que el tomcat inicie automáticamente o manualmente.
4. El jdk y el jre se encuentra en /opt/java1.5 y /opt/java1.5/jre respectivamente.
5. En la carpeta del tomcat se encuentran las siguientes carpetas:
   a. webapps: en esta carpeta se pone el “.war” que se va a desplegar.
   b. logs: en esta carpeta se encuentra los logs del tomcat.
   c. conf: en esta carpeta se encuentran los ficheros de configuración.
   d. bin: en esta carpeta se encuentran los binarios del tomcat.
   e. temp: en esta carpeta se encuentran los ficheros temporales del tomcat

Una vez conocido esto se procede a la configuración del Tomcat 5.5.20.

1. Ir al profile del usuario que va a ejecutar el tomcat y poner estas variables de ambiente:
   a. $ vi /.profile
   b. JAVA_HOME="/opt/java1.5"; export JAVA_HOME
   c. JRE_HOME="/opt/java1.5/jre"; export JRE_HOME
   d. CATALINA_HOME="/opt/hpws/tomcat"; CATALINA_HOME
   e. CATALINA_BASE="/opt/hpws/tomcat"; export CATALINA_BASE
   f. En la variable PATH añadir esto al final, usando los dos puntos como enlace /opt/hpws/tomcat/bin:/sbin/init.d

2. Es aconsejable no iniciar el tomcat por el usuario root, ya que este usuario tiene privilegios de **SUPERUSUARIO** y cualquier fallo podría incidir sobre otra configuración, el usuario que se aconseja para eso es el www.
3. El fichero catalina.out que se encuentra en $ /opt/hpws/tomcat/logs hay que crearlo nuevamente porque tiene errores en la instalación inicial.
   a. $ rm /opt/hpws/tomcat/logs/catalina.out (se elimina el fichero)
   b. $ touch /opt/hpws/tomcat/logs/catalina.out (se crea el fichero nuevo)
   c. $ chown -R www:users /opt/hpws/tomcat/logs (se cambia el usuario con permisos para la carpeta logs)
   d. $ chmod -R 744 /opt/hpws/tomcat/logs/ (se cambia la permisología a la carpeta logs)
4. A la carpeta work:
   a. $ chown -R www:users /opt/hpws/tomcat/work (se cambia el usuario con permisos para la carpeta work)
   b. $ chmod -R 755 /opt/hpws/tomcat/work (se cambia la permisología a la carpeta work)
5. En el fichero web.xml y server.xml hay que añadir esta configuración para que pueda levantar la aplicación del proyecto.
   a. $ vi /opt/hpws/tomcat /conf/web.xml (se edita el fichero web.xml)
      i. En el tercer servlet que sale añadir esto entre las etiquetas <servlet></servlet>

```
<init-param>
<param-name>mappedfile</param-name>
<param-value>true</param-value>
</init-param>
<init-param>
<param-name>compilerTargetVM</param-name>
<param-value>1.5</param-value>
</init-param>
<init-param>
<param-name>compilerSourceVM</param-name>
<param-value>1.4</param-value>
</init-param>
<load-on-startup>3</load-on-startup>
```

   b. $ vi /opt/hpws/tomcat/conf/server.xml (se edita el fichero server.xml)
      i. Buscar el siguiente comentario

         <! -- Define a non-SSL HTTP/1.1 Connector on port 8081 -->

         y en <Conector port=”….. ” Establecer el puerto por el que se quiere que levante la aplicación.
6. Editar el fichero tomcat-users.xml, en este fichero se encuentran los usuarios con permisos para la interfaz web del tomcat
   a. $ vi /opt/hpws/tomcat/conf/ tomcat-users.xml

b. Sustituir el usuario hpux por el de admin-cicpc y establecer un password para el usuario.

7. Cambiar la permisos a la carpeta conf del tomcat
   a. $ chown -R www:users /opt/hpws/tomcat/conf (se cambia el usuario con acceso a la carpeta)
   b. $ chmod -R 755 /opt/hpws/tomcat/conf (se cambia la permisología de la carpeta)
8. Editar el fichero setenv.sh que se encuentra en $ /opt/hpws/Tomcat/bin/
   a. $ vi /opt/hpws/tomcat/bin/setenv.sh
   b. En la variable JAVA_OPTS poner al principio esta configuración

   -Xms756m -Xmx2048m -XX:PermSize=256m -XX:MaxPermSize=512m
   c. Los parámetros -Xms, -Xmx, -XX:PermSize y -XX:MaxPermSize significan:
      i. -Xms: menor tamaño posible de la memoria reservada.
      ii. -Xmx: mayor tamaño posible de la memoria reservada.
      iii. -XX:PermSize: menor tamaño dedicado a la generación permanente.
      iv. -XX:MaxPermSize: mayor tamaño dedicado a la generación permanente.

   La generación permanente no es más que el espacio dedicado para instanciar las clases que la aplicación va a utilizar y que no van a cambiar durante la ejecución de la misma.
9. Hacer una prueba para ver si está bien la configuración y ver si no tiene errores
   a. $ /opt/hpws/tomcat/bin/catalina.sh run –security
   b. Verificar en la consola que no hay errores, los errores se muestran con una etiqueta **SEVERE**.
   c. Si no hay errores se pasa a probar el tomcat, para esto se abre un navegador web y se pone en la barra de dirección

      http://ip-del-servidor:puerto
   d. Si levanta bien el servidor se pasa a detener el servicio para seguir con la configuración.

      /opt/hpws/tomcat/bin/catalina.sh stop –force
10. Vamos a la carpeta /etc/rc.config.d para que se inicie automáticamente el servicio
    a. Editar el fichero hpws_tomcatconf
       i. $ vi /etc/rc.config.d/ hpws_tomcatconf
    b. Cambiar el valor de HPWS_TOMCAT_START a 1

Una vez terminada la configuración inicial del tomcat se pasa ahora a vincularlo con SSL. Primeramente dar una introducción a que es SSL y que son los Certificado Digitales.

ANEXOS.

SSL o “Secure Socket Layer” provee una "capa" para asegurar los protocolos de Internet y prevenir que la información transmitida por ellos sea falsificada, modificada o interceptada por terceras personas mientras se encuentra en tránsito por la red.
SSL opera mediante el intercambio de llaves entre el cliente y el servidor para poder descifrar la información que ha sido codificada por un “cipher simétrico”. Lo que esto significa es que los datos encriptados solo pueden ser desencriptados por el poseedor de la llave correcta.
Los Certificados Digitales son una forma de agregar un tercer "árbitro" a la cadena de confianza de la comunicación por SSL. Lo que un certificado digital hace es agregar el "endoso" de un tercero que garantiza la integridad, y existencia de la organización que envía los datos. Esto significa que una autoridad certificadora avala que la empresa que es dueña del sitio web, por ejemplo, realmente existe.

Un certificado digital que siga el estándar X509v3, utilizado por los navegadores, contiene la siguiente información:

- Identificación del titular del certificado: Nombre, dirección, entre otros.
- Clave pública del titular del certificado.
- Fecha de validez.
- Número de serie.
- Identificación del emisor del certificado.

Viendo anteriormente una breve introducción a SSL y Certificados Digitales se pasa a explicar en detalles como vincular el Tomcat con SSL.

1. Este comando crea un nuevo fichero llamado “*.keystore” en el “Home Directory” del usuario que lo está ejecutando. Para especificar un directorio diferente se añade el parámetro –keystore seguido de la dirección completa en donde se quiere guardar el fichero “*.keystore”.
   a. $ /opt/java1.5/bin/keytool –genkey –alias tomcat –keyalg RSA \
      -keystore /camino/al/*.keystore

      En este comando se ve como en el alias se especifica que es para el tomcat y también la elección del algoritmo de encriptación es el RSA.
2. Después de ejecutar este comando, nos va a salir en pantalla un cartel pidiendo el “keystore password”. El “keystore password” por defecto usado por el Tomcat es “changeit” (todo en minúscula).

3. Después de entrado el “keystore password” se nos pide información general acerca del Certificado Digital que se crea, por ejemplo:
   a. Al final se da “Enter” porque el password es el mismo que el “keystore password”.
4. Ahora se edita el fichero server.xml para habilitar la conexión https al tomcat.
   a. $ vi /opt/hpws/tomcat/conf/server.xml
   b. Se busca el comentario

   <! -- Define a SSL HTTP/1.1 Connector on port 8443 -->
   c. Quitamos los indicadores de comentario para habilitar la conexión y se añade esto dentro de la etiqueta <Conector

   keystorePass="changeit” keystoreFile="/opt/hpws/tomcat/ssl/CICPC.keystore"
5. Finalmente se reinicia el tomcat para que vea los últimos cambios efectuados.

[Anexo 2]. Instalación y configuración del SubVersioN.

Instalación.

1. Instalar SubVersioN: # apt-get install subversion
2. Instalar apache y módulos necesarios: # apt-get install apache2 libapache_svn
3. Habilitar módulos del Apache:

Módulos necesarios:

- dav
- dav_fs
- dav_svn
- authnz_svn

Adicionalmente:

- ldap
- authz_ldap

a2enmod dav dav_fs dav_svn authz_svn

Habilitando dav como una dependencia: # a2enmod dav_fs

Módulo dav_fs instalado, ejecutar /etc/init.d/apache2 force-reload para habilitarlo.

a2enmod dav_svn

a2enmod authz_svn

Habilitando ldap como una dependencia: # a2enmod ldap authnz_ldap

Módulo ldap instalado, ejecutar /etc/init.d/apache2 force-reload para habilitarlo.

Módulo authnz_ldap instalado; ejecutar /etc/init.d/apache2 force-reload para habilitarlo.

Configuración.

1. Crear carpeta raíz de repositorios

mkdir /media/svn/svnroot

mkdir /media/svn/svnroot/repn

2. Crear repositorios nuevos

svnadmin create /media/svn/svnroot/repn

3. Copiar repositorios antiguos

cp -r <camino> /media/svn/svnroot/portalweb

cp -r <camino> /media/svn/svnroot/arquitectura

4. En caso de que exista un antiguo repositorio, copiarlo como solo lectura:

mkdir /media/bkp/svnroot

chown -R www-data:admin /media/bkp/svnroot

chmod -R 775 /media/bkp/svnroot

Copiar los archivos:

cp -r <camino> /media/svn/svnroot/"viejo repositorio"

Una vez copiados ponerlo solo lectura:

chown -R www-data:admin /media/bkp/svnroot

chmod -R 555 /media/bkp/svnroot

Hacer vínculo simbólico:

ln -s /media/bkp/svnroot/"viejo repositorio" /media/svn/svnroot/

5. Establecer los permisos a los archivos

chown -R www-data:admin /media/svn/svnroot

chmod -R 775 /media/svn/svnroot

6. Crear archivos de configuración

mkdir /etc/apache2/svn-conf/

touch /etc/apache2/svn-conf/dav_svn.authz

touch /etc/apache2/svn-conf/dav_svn.passwd

6.2 Crear el primer usuario del repositorio para autenticación por ficheros:

htpasswd -c /etc/apache2/svn-conf/dav_svn.passwd admin

New password: (cicpc2svn)

Re-type new password: (cicpc2svn)

"Adding password for user admin"

6.3 Crear el archivo de asignación de permisos

vi /etc/apache2/svn-conf/dav_svn.authz

7. Configurar el sitio del svn.

Modificar el archivo:

/etc/apache2/conf/mods-enabled/dav_svn.conf

con el siguiente contenido:

<Location /svn>

DAV svn

SVNParentPath /media/svn/svnroot
SVNListParentPath on
AuthType Basic
AuthBasicProvider file ldap
AuthName "Repositorio SVN - Proyecto CICPC"
AuthUserFile /etc/apache2/svn-conf/dav_svn.passwd
AuthzSVNAccessFile /etc/apache2/svn-conf/dav_svn.authz
AuthLDAPURL "ldap://10.0.0.3/OU=UCI
Domain Users, DC=uci, DC=cu?sAMAccountname?sub?(objectClass=person)"
AuthLDAPBindDN "ad.search@uci.cu"
AuthLDAPBindPassword "uF2SODWAHiW0eJboFFQEAvVzJ"
AuthzLDAPAuthoritative Off
Require ldap-group OU=UCI Domain Users,DC=uci,DC=cu
Require valid-user
Order Deny, Allow
Deny from all
Allow from 10.35.
</Location>
8. Poner en funcionamiento el repositorio
8.1 Reiniciar el Apache
/etc/init.d/apache2 restart
Nota: si el Apache muestra una alerta de que no encuentra el ServerName, se debe modificar el archivo
/etc/apache2/conf/apache2.conf
y adicionar la siguiente línea:
ServerName “nombre del servidor”

[Anexo 3]. Instalación del Trac con Python 2.5.1

Archivos y Carpetas del Trac:
/etc/trac
/etc/apache2/sites-enabled/trac
/etc/apache2/sites-available/trac
/usr/share/trac
/usr/share/doc/trac
/usr/share/python-support/trac
/usr/share/python-support/trac/trac
/var/trac

/var/lib/python-support/python2.5/trac

Personalizadas:

/var/lib/mysql/trac

/var/smb/trac

Ficheros de configuración:

/etc/apache2/sites-enabled/trac

/etc/apache2/trac-conf/ trac.passwd: usuarios y contraseñas para autenticación contra ficheros

/etc/apache2/trac-conf/trac.authz: grupos y usuarios miembros

/var/trac/<nombre-proyecto>/conf/trac.ini

Carpetas de la aplicación:

/var/lib/python-support/python2.5/trac: archivos de la aplicación Trac compilados (.pyc)

/usr/share/python-support/trac/trac: archivos de la aplicación Trac compilados python (.py)

Carpetas del proyecto:

/var/trac/<nombre-proyecto>: raíz del proyecto

Instalación.

Dependencias

- subversion
  - libsvn1 (se instala automáticamente junto con subversion)
- python
  - python-subversion
  - python-setuptools.
  - python-mysqldb: (Interfaz Python para MySQL)
- apache2
  - libapache2-mod-python
  - libapache2-svn
- mysql

1. Instalar Python bindings para Subversion.

apt-get install python-subversion

1.2 Instalar mod_python

apt-get install libapache2-mod-python libapache2-mod-python-doc

a2enmod mod_python

1.3 Instalar el Trac

apt-get install trac

Además serán instalados los siguientes paquetes:

- python-clearsilver
- python-pysqlite2

ANEXOS.

Adicionalmente son necesarios instalar:

apt-get install python-setuptools

apt-get install python-mysqldb

2. Crear carpeta raíz de proyectos

mkdir /var/trac

3. Crear base de datos

Se crea una base de datos 'trac' en el mysql local y un usuario 'trac' y contraseña 'traccicpc' y se le asignan derechos a este usuario sobre la base de dados 'trac' creada

3. Crear el proyecto

trac-admin /var/trac/cicpc initenv

Project Name [My Project]> CICPC

Database connection string [sqlite:db/trac.db]> mysql://trac:traccicpc@localhost:3306/trac

(Previamente se debe crear esta base de datos en el MySQL)

Repository type [svn]>: (por defecto)

Camino al repositorio [/path/to/repos]> /media/svn/svnroot/arquitectura

Directorio de plantillas [/usr/share/trac/templates]>: (por defecto)

Otra manera es pasarle todos los parámetros:

trac-admin /var/trac/cicpc initenv CICPC mysql://trac:traccicpc@localhost:3306/trac svn /media/svn/svnroot/arquitectura /usr/share/trac/templates

3.1 Establecer permisos de escritura en la carpeta del proyecto

chown -R www-data:admin /var/trac/cicpc/

chmod -R 775 /var/trac/cicpc/

3.2 Modificar el fichero /var/trac/cicpc/conf/trac.ini

Modificar las siguientes líneas:

[browser]

downloadable_paths = /trunk, /branches/*, /tags/*

downloadable_paths = /ArquitecturaCICPC

[header_logo]

link = http://10.35.11.32/trac/cicpc

[timeline]

default_daysback = 1

[trac]

database = mysql://trac:traccicpc@localhost:3306/trac

repository_dir = /media/svn/svnroot/arquitectura

Notar que en este caso dentro del repositorio arquitectura existe una carpeta ArquitecturaCICPC donde se encuentra el proyecto.

5. Sincronizar el trac con el repositorio

trac-admin /var/trac/cicpc resync

Nota: demora un tiempo en dependencia de la cantidad de versiones que ya tenga el repositorio.

6. Configurar el sitio del trac en el Apache

6.1 Crear el sitio trac en el apache

touch /etc/apache2/sites-available/trac

Modificar el fichero /etc/apache2/sites-enabled/trac

```
<Location /mpinfo>
   SetHandler mod_python
   PythonHandler mod_python.testhandler
</Location>
<Location /trac>
   SetHandler mod_python
   PythonHandler trac.web.modpython_frontend
   PythonOption TracEnvParentDir /var/trac
   PythonOption TracUriRoot /trac
   SetEnv PYTHON_EGG_CACHE /var/cache/python-egg
</Location>
<LocationMatch "/trac/[^/]+/login">
   AuthType Basic
   AuthBasicProvider file ldap
   AuthName "TRAC - Proyecto CICPC"
   AuthUserFile /etc/apache2/trac-conf/trac.passwd
   AuthGroupFile /etc/apache2/trac-conf/trac.authz
   AuthLDAPURL "ldap://10.0.0.3/OU=UCI
Domain Users, DC=uci, DC=cu?sAMAccountname?sub?(objectClass=person)"
   AuthLDAPBindDN "ad.search@uci.cu"
   AuthLDAPBindPassword "uF2SODWAHiW0eJboFFQEAvVzJ"
   AuthzLDAPAuthoritative Off
#   Require valid-user
   Require group proyecto
</LocationMatch>
```

Para habilitar la autenticación contra dominio se debe tener habilitado el modulo ldap

a2enmod ldap

a2enmod authnz_ldap

Módulos habilitados:

alias, auth_basic, authn_file, authnz_ldap, authz_default, authz_groupfile, authz_host, authz_user, autoindex, cgi, dav, dav_svn, dir, env, expires, ldap, mime, mod_python, negotiation, php5, rewrite, setenvif, status.

6.2 Crear los archivos de acceso

mkdir /etc/apache2/trac-conf

6.2.1 Crear el archivo de acceso

vi /etc/apache2/trac-conf/trac.authz

Para crear el archivo de autenticación usuarios locales y el usuario admin:

htpasswd -c /etc/apache2/trac-conf/trac.passwd admin

New password: (cicpc2trac)

Re-type new password: (cicpc2trac)

Una vez creado se pueden adicionar más usuarios de la siguiente manera:

htpasswd /etc/apache2/trac-conf/trac.passwd usuario1

6.3 Habilitar el sitio

a2ensite trac

/etc/init.d/apache2 reload

7. Establecer los permisos de los usuarios del trac

trac-admin /var/trac/cicpc

8. Adicionar componentes:

trac-admin /var/trac/cicpc/ component add "Componente de Solicitudes" admin

8.1 Ver componentes

trac-admin /var/trac/cicpc/ component list

Referencia:

$ trac-admin --help

9. Instalación de Plugins

URL: http://trac.edgewall.org/wiki/PluginList

9.1 Configurar Plugin Cache

Crear el archivo de cache de los Python eggs

mkdir /var/cache/python-egg

chown -R www-data:admin /var/cache/python-egg

chmod -R 775 /var/cache/python-egg

Notar que ya se había declarado el directorio para la cache de los Python egg en las configuraciones del sitio trac (/etc/apache2/sites-available):

```
<Location /trac>
  SetEnv PYTHON_EGG_CACHE /var/cache/python-egg
</Location>
```

Algunas bibliografías utilizan la dirección /var/www/.python-eggs en lugar de la anterior.

9.2 RPC XML-RPC plugin

URL http://trac-hacks.org/wiki/XmlRpcPlugin

Archivo: xmlrpcplugin.zip

Copiarlo en la raíz de plugins del proyecto /var/trac/cicpc/plugins/.

Darle permisos de ejecución:

chmod +x /var/trac/cicpc/plugins/xmlrpcplugin.zip

Supuestamente instalaría así:

easy_install -Z /var/trac/cicpc/plugins/xmlrpcplugin.zip/0.10

error: “Not a URL, existing file, or requirement spec:”
'/var/trac/cicpc/plugins/xmlrpcplugin.zip/0.10'

Descompactar e instalar:

cd /var/trac/cicpc/plugins

unzip /var/trac/cicpc/plugins/xmlrpcplugin.zip

easy_install /var/trac/cicpc/plugins/xmlrpcplugin/0.10/

Habilitar el plugin en el trac.ini adicionando:

[components]
tracrpc.* = enabled

9.3 CruiseControl

URL https://oss.werkbold.de/trac-cc/

En nuestro caso el CruiseControl con un proyecto llamado 'cicpc' está corriendo en un servidor con Windows, por lo que como el Trac necesita acceso a los ficheros del CruiseControl hay que compartir estas carpetas y montarlas en el filesystem local.

9.3.1 Crear usuario 'cruisecontrol' con contraseña 'cruisecontrol' con acceso de lectura a la carpeta del CruiseControl.

9.3.2 Instalando el CruiseControl en C:\CruiseControl\ y el proyecto llamado cicpc, entonces compartir las carpetas:

C:\CruiseControl\webapps\cruisecontrol\xsl

C:\CruiseControl\logs\cicpc

9.3.3 Crear en el servidor Linux los puntos de montura:

mkdir /mnt/cruisecontrolXsl

mkdir /mnt/cruisecontrolLogs

Modificar el fstab para que monte las carpetas compartidas desde que inicie el sistema.

// servidorCruiseControl /xsl /mnt/cruisecontrolXsl smbfs
ro,auto,iocharset=utf8,codepage=unicode,unicode,username=cruisecontrol,password=cruise
control,workgroup=10.35.12.150 0 0

//servidorCruiseControl/logs /mnt/cruisecontrolLogs smbfs ro,auto,iocharset=utf8,codepage=unicode,unicode,username=cruisecontrol,password=cruisecontrol,workgroup=10.35.12.150 0 0

mount -a -t smbfs

Programar el cron para que remonte los recursos remotos periódicamente.

crontab -e

*/10 * * * * mount -a -t smbfs

9.3.4 Instalar el plugin TracCC-0.1.3-py2.4.egg

Archivo: TracCC-0.1.3-py2.4.egg

Copiarlo en la raíz de plugins del proyecto /var/trac/cicpc/plugins/.

Darle permisos de ejecución:

chmod +x /var/trac/cicpc/plugins/xmlrpcplugin.zip

cd /var/trac/cicpc/plugins/

easy_install /var/trac/cicpc/plugins/TracCC-0.1.3-py2.5.egg

9.3.5 Configurar el trac.ini

Adicionar en la sección components:

[components]

traccc.* = enabled

y al final del archivo:

[cruisecontrol]

ccpath = /mnt/cruisecontrolLogs

buildstatusfile = status.txt

xslfile = /mnt/cruisecontrolXsl/buildresults.xsl

Luego se reinicia el apache

Tratamos de ver si el Trac está funcionando y si se da clic en la pestaña CruiseControl se muestra el siguiente error:

Internal Server Error

500 Internal Server Error (libxml and libxslt is not installed.)

Si esto ocurre es que no están instaladas las librerías necesarias libxml2 y libxslt con sus Python bindings.

- libxslt1.1, libxml2, python-libxslt1, python-libxml2

Verificando:

dpkg --get-selections | grep libxml

libxml-parser-perl install

libxml-twig-perl install

libxml2 install

libxml2-utils install

python-libxml2 install

dpkg --get-selections | grep libxsl

libxslt1.1 install

dpkg --get-selections | grep python-libxml

python-libxml2 install

Finalmente

dpkg --get-selections | grep python-libxsl

Como falta la librería python-libxsl se debe instalar.

Ver la lista de software disponible:

apt-cache pkgnames | grep python-libxsl

python-libxslt1

python-libxslt1-dbg

Instalar

apt-get install python-libxslt1

Ya se puede actualizar la página del CruiseControl y funcionará.

[Anexo 4]. Modelo 1: Planificación del Tiempo de Máquina.

Semana X – XX		**Mes:** XX	**Año:** XX	**Solicita:** XXX	
No	**Rol**	**Nombre y Apellidos**		**Turno**	**Restricciones a tener en cuenta**

[Anexo 5]. Modelo 2: Libro de Incidencias.

No. De Inventario del Recurso.	**Fecha**	**Hora**	**Observaciones**	**Nombre y Firma**

ANEXOS.

[Anexo 6]: Modelo 3: Libro de Visita.

No. De Pase	**Fecha**	**Nombre y Apellidos**	**Centro de Trabajo**	**Hora de Entrada**	**Hora de Salida**	**Objetivo de la visita**	**No. CI.**	**Autorizado por:**

[Anexo 7]. Modelo 4: Solicitud de Mantenimiento.

Fecha: dd-mm-aa	**PC No**: XX	Hardware ____ Software ____
Nombre del que solicita: nombre y rol		
Descripción del Problema o la necesidad:		
Ejemplo: Necesito Instalar el Microsoft Visio que trae la instalación del Office *Ejemplo: El eclipse no levanta cuando estoy en mi sesión de trabajo.* *Ejemplo: la máquina se reinicia cada 20 min.*		
Solicitud atendida por: nombre del jefe de sistema		**Estado:** (no resuelta, resuelta, en proceso, esperando por otra persona, aplazada)

[Anexo 8]. Modelo 5: Registro de soportes magnéticos.

· No. Consecutivo en el registro	
· Contenido fundamental del soporte	
· Trabajo para el que se destina	
· Grado de clasificación de la información	
· Nivel de acceso del soporte	
· Fecha y hora de entrada	
· Fecha y hora de baja	
· Observaciones	

ANEXOS.

[Anexo 9:]. Modelo 6: Registro de entrega/recepción de soportes magnéticos.

· No. Del soporte magnético	
· Contenido fundamental del soporte	
· Entrega:	
· Nombre y firma de quién entrega el soporte	
· Nombre y firma de quién recibe el soporte	
· Objetivo de utilización del soporte	
· Conservación de la relación interna	
· Fecha y hora de entrega	
· Recepción	
· Nombre y firma de quién devuelve el soporte	
· Nombre y firma de quién recibe el soporte	
· Resultado de la comprobación contra la relación interna	
· Resultado de la revisión contra virus	
· Fecha y hora de recepción	