HERRAMIENTA PARA GESTIONAR Y CONTROLAR POLITICAS DE SEGURIDAD INFORMATICA. “HEGCON-PS”

SANTANDER ALFONSO OLIVERO MARQUEZ
GUILLERMO EDUARDO JURADO FAJARDO

UNIVERSIDAD DEL CAUCA
FACULTA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
POPAYÁN

HERRAMIENTA PARA GESTIONAR Y CONTROLAR POLITICAS DE SEGURIDAD INFORMATICA. "HEGCON-PS"

SANTANDER ALFONSO OLIVERO MARQUEZ

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR EL TITULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

INGENIERO ESPECIALISTA SILER AMADOR DONADO
DIRECTOR

UNIVERSIDAD DEL CAUCA
FACULTA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
POPAYÁN
2003

HERRAMIENTA PARA GESTIONAR Y CONTROLAR POLITICAS DE SEGURIDAD INFORMATICA. "HEGCON-PS"

GUILLERMO EDUARDO JURADO FAJARDO

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR EL TITULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

INGENIERO ESPECIALISTA SILER AMADOR DONADO
DIRECTOR

UNIVERSIDAD DEL CAUCA
FACULTA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
POPAYÁN
2003

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Popayán 3 de Diciembre del 2003

A Dios le doy gracias por permitirme llegar donde me encuentro..,

A mi querido Padre Santander, mi adorada Madre Mercedez, mis bellos Hermanos javier, stella, roberto, milena,richar, dany, patricia, sobrinos y cuñadas. En especial a mi hermana Stella quien simpre me apoyo y me brindo su luz en mis momentos de oscuridad.

A mi abuela idolina, mi abuelo santander y mi abuela juana, que aunque estan lejos siempre habitarán en mi corazon y mi mente.

A mi novia Alba Lucia que con su amor, comprensión, paciencia y dedicación es un pilar fundamental en mi vida para lograr las metas deseadas.

A mis amigos, Guillermo, Ramon, Juan Pablo, Franklin, jorge padilla, jose antonio, jhon y en especial Leyis Lubo que me brindo todo su apoyo y colaboración para cumplir esta meta.

Santander Olivero M.

A mis Padres Guillermo Jurado y Lidia Fajardo, por haber hecho por mí Siempre, mas de lo necesario

A nkt, por protagonizar a mi lado la difícil tarea de enfrentarse a diario a esta "Matrix" de la vida…

Y sobretodo a Dios, porque lo que soy, tengo y hago no es suficiente para demostrarle lo importante que es en mi vida… antes solo respiraba, ahora por su Verdad tengo Vida…

"la cuchara no existe…"

Guillermo Eduardo Jurado Fajardo

AGRADECIMIENTOS

A Siler A., Santander O., Juan Carlos V., Luis Ernesto G.,

Libardo P., Andrés F., por ayudarnos a llevar este proyecto

A sus posibles límites…

Al mundo Hacker y los "Habitantes del Underground",

Por estar siempre ahí, aunque nadie

Se dé cuenta…

nkt

Listado de Figuras

Figura 1. Estructura jerárquica de la seguridad en la información.[4] 38
Figura 2. Diagrama Conceptual del Sistema Hegcon-PS 106
Figura 3. Interfaz de Administración del Gestor 107
Figura 4. Módulo de Gestión de Políticas de Seguridad 112
Figura 5. Visualizador Políticas de Seguridad Implementadas 113
Figura 6. Descriptor de Políticas en LPS 114
Figura 7. Informes y reportes del sistema Hegcon-PS 115
Figura 8. Proceso de edición manual de archivos 117
Figura 9. Definición de la configuración para la comunicación Gestor/Agente. 119
Figura 10. Personalización de la interfaz de Hegcon-PS 120
Figura 11. Opción de Configuración de la Seguridad 121
Figura 12. Envió de tareas On-Line 123
Figura 13. Ayuda de Hegcon-PS 124
Figura 14. Interfaz de ejecución de una política. 130
Figura 15. Interfaz de información al ejecutar la política control software. 131
Figura 16. Ejecución del Agente en Modo Verbose 134

LISTADO DE TABLAS

Tabla 1. Resumen del valor riesgo anual en la Universidad del Cauca

Tabla 2. Clasificación de una política de seguridad

Tabla 3. Clasificación de la política informática de acuerdo al recurso dirigido

Tabla 4. Resultados de los análisis de riesgo [2].

Tabla 5. Descripción de los componentes para crear una política en el gestor

Tabla 6. Naturaleza de las política a implementar en Hegcon-PS

Tabla 7. Criterios de selección usados para la clasificación de las políticas en Hegcon-PS.

Tabla 8. Políticas implementadas en Hegcon-PS

Tabla 9. Objetivos y sanciones generales de las políticas implementadas en Hegcon-PS

Tabla 10. Valoración de riesgos de la política de Agentes de Control

Tabla 11. Estrategias de seguridad e Implementación para la política de operación de los Agentes de control

Tabla 12. Valoración de riesgos de la política de monitoreo de software.

Tabla 13. Estrategias de seguridad e Implementación para la política de monitoreo

Tabla 14. Valoración de riesgos de la política control de visitas a sitios Web no autorizados

Tabla 15. Estrategias de seguridad e Implementación para la política control de visitas a sitios.

Tabla 16. Valoración de riesgos de la política que implementa mecanismos de Protección contra virus Informáticos.

Tabla 17. Estrategias de seguridad para la política de Protección contra Virus Informáticos

Tabla 18. Valoración de riesgos de la política que implementa mecanismo de control sobre los recursos compartidos.

Tabla 19. Estrategias de seguridad e Implementación para la política control de

Lista de Anexos

Anexo A. Definición de los distintos Virus informáticos.

Anexo B. Estructura de los lenguajes de programación.

Anexo C. Modelado de Hegcon-ps.

CONTENIDO

1. INTRODUCCION 4

1.1. VISIÓN HISTÓRICA: 5

1.2. ANTECEDENTES 7

1.2. FUNCIONALIDAD DEL SISTEMA HEGCON-PS 12

1.3. AMBIENTE DE DESARROLLO DEL SISTEMA HEGCON-PS 13

1.4. PROPÓSITOS PRINCIPALES DEL PROYECTO 16

2. FUNDAMENTOS DE SEGURIDAD EN REDES INFORMATICAS 17

2.1. LA SEGURIDAD INFORMÁTICA. 17

2.2. SEGURIDAD FÍSICA 19

2.3. SEGURIDAD LÓGICA 21

2.4. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA 23

2.5 RIESGOS Y AMENAZAS 26

3. POLITICAS INFORMATICAS: CONCEPTOS Y ESTRUCTURA 33

3.1 DEFINICIÓN DE POLÍTICA DE SEGURIDAD 33

3.2. IMPORTANCIA DE LAS POLÍTICAS DE SEGURIDAD 34

3.3. CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA 35

3.4. ESTRUCTURA DE LAS POLÍTICAS DE SEGURIDAD 36

3.5. DESCRIPCIÓN DE LAS POLÍTICAS PILOTO IMPLEMENTADAS. 41

3.6. ESTRATEGIAS DE SEGURIDAD 44

3.7. NATURALEZA DE LAS POLÍTICAS DE SEGURIDAD 49

4. PSEUDO-LENGUAJE DE OPERACIÓN 64

4.1. DEFINICIÓN LENGUAJE DE POLÍTICAS DE SEGURIDAD (LPS) 67

4.2. INTRODUCCIÓN. 67

4.3 REGLAS DE PRODUCCIÓN PARA LENGUAJE DE POLÍTICAS DE SEGURIDAD (LPS) 78

4.4 GRAMÁTICA LPS PARA LAS OPERACIONES EN LPS 79

4.5. SINTAXIS PARA LAS OPERACIONES EN LPS 86

4.6. IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD EN EL PROYECTO HEGCON-S 99

5. MÓDULO DE GESTIÓN. GESTOR 105

5.1 LAS FUNCIONES PRINCIPALES DEL GESTOR 105

5.2 DISEÑO DEL MÓDULO DE GESTIÓN 107

5.4 ACTIVIDADES DE GESTIÓN 109

6. MODULO DE CONTROL. AGENTE 127

6.1. FUNCIONES DEL AGENTE 127

6.2. OPERACIÓN DEL AGENTE. 129

6.3. CONFIGURACIÓN DEL AGENTE 133

7. RESULTADOS 136

CONCLUSIONES 138

RECOMENDACIONES 140

GLOSARIO 142

BIBLIOGRAFÍA Y REFERENCIAS 147

1. INTRODUCCION

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información al igual que servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

De acuerdo con lo anterior, para implementar políticas de seguridad se requiere de un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, además de constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Este trabajo de grado implementa un sistema de gestión y control para las políticas informáticas en una organización (Hegcon-PS)[1]. En este se busca sea utilizada en la red

[1] Hegcon-PS. Herramienta de Gestión y Control de Políticas de Seguridad Informática

de datos de la universidad del cauca. Se desea iniciar un proceso educativo y de concientización sobre el cumplimento de las políticas de seguridad informáticas por parte de los usuarios de la red de datos.

Este proyecto tiene un carácter totalmente educativo, y no es su intención generar directivas de tipo restrictivo que lleguen a atentar contra el libre uso de los recursos de red por parte de los usuarios ni generar polémicas en torno a asuntos sobre los cuales todavía no existe una reglamentación legal, penal y judicial que se puedan aceptar como parámetros de referencia.

Hegcon-PS permite automatizar la planificación, creación y el cumplimiento de las políticas de seguridad informática de una organización, con ahorros significativos en tiempo y dinero ya que elimina las actividades repetitivas y redundantes asociadas con estas tareas, evitando así los errores humanos que comúnmente aparecen al delegar las mismas a empleados de la organización.

Es de anotar que el desarrollo de las políticas de seguridad se está llevando a cabo en un proceso paralelo a este proyecto. Una vez culminadas las políticas de seguridad y terminado el proceso educativo el producto está abierto para ser escalable[2] y contar con la capacidad de hacer cumplir la políticas impuesta por la institución mediante un proceso restrictivo. Este es un trabajo que refleja la realidad que estamos viviendo en Colombia y el mundo, “Hay que educar para prevenir incidentes lamentables y estar protegidos para evitar ser violentados”.

1.1. Visión Histórica:

La "Seguridad es una necesidad básica. Estando interesada en la prevención contra daños para la vida y las posesiones es tan antigua como ella”[1] .

[2] Escalable: Que se puede mejorar su configuración.

Como todo concepto, la seguridad se ha desarrollado y ha emergido una evolución dentro de las organizaciones sociales.

La primera evidencia de una cultura y organización en seguridad "madura" aparece en los documentos de la Res Publica (estado) de Roma Imperial y Republicana.
El próximo paso de la seguridad fue la especialización. Así nace la seguridad externa (aquella que se preocupa por las amenazas de los entes externos hacia la organización); y la seguridad interna (aquella preocupada por las amenazas de nuestra organización con la organización misma): De estos dos se pueden desprender la seguridad privada y pública al aparecer el estado y depositar su confianza en unidades armadas.

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdida han traído nueva luz a los sistemas de seguridad.

La seguridad moderna se origino con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayor en 1919, identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad fayor dice "...Salvaguardar propiedades y personas contra el robo, fuego, inundaciones, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Todas las medidas para conferir la requerida paz y tranquilidad al personal".

Las medidas de seguridad a las que se refiere Fayor, solo se restringían a los exclusivamente físico de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "Cerebros Electrónicos", esta mentalidad se mantuvo, ya que se preguntaban "¿Quien seria capaz de entender estos

complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?"[2] .

Desde el punto de vista técnico, la seguridad esta en manos de la dirección de la organizaciones, en ultima instancia en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

1.2. Antecedentes

El fenómeno de la Internet se ha extendido a gran velocidad y en grandes proporciones, presentándose en su seno un sin numero de situaciones sorprendentes y muy difíciles de imaginar hace solo unos años.

Inicialmente Internet nace como una serie de redes que promueven el intercambio de información entre investigadores que colaboran en proyectos conjuntos o comparten resultados usando los recursos de la red.

En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos sensibles o clasificados que pudieran manejar los usuarios. Situación esta muy común, pues hay que recordar que la Internet nace como un contrato del Departamento de Defensa Americano -año 1968- para conectar entre sí tanto las Universidades como los centros de investigación que colaboran de una manera u otra con las Fuerzas Armadas Norteamericanas.

Los protocolos[3] de Internet fueron creados de una forma deliberada para que fueran simples y sencillos. El poco esfuerzo realizado para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los

[3] protocolo: conjunto de normas y procedimientos útiles para la transmisión de datos, conocido por el emisor y el receptor: protocolo de corrección de datos.

niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

Más recientemente, la conexión de las redes empresariales y educativas a redes públicas como Internet, Compuserver, etc., se ha producido a un ritmo vertiginoso muy superior a la difusión de ninguna otra tecnología anteriormente ideada. Ello ha significado que esta red de redes se haya convertido en "la red" por excelencia.

De igual forma la seguridad se ha convertido en un problema realmente serio a pesar que los horizontes de oportunidades ha sido ampliado a millones de clientes potenciales, también han crecido considerablemente los atacantes, con todos los inconvenientes que este suceso conlleva se ha convertido en el medio más popular de interconexión de recursos informáticos y embrión de las anunciadas autopistas de la información.

Se ha incrementado la variedad y cantidad de usuarios interconectados a la red con fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la cooperación altruista, la práctica política o, simplemente, el juego. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas

Debido a la complejidad y extensión de la red se dificulta la ubicación, detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo diariamente en los sistemas informáticos. Es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la realización de todos los procesos de seguridad informáticos al pie de la letra y el continuo control y vigilancia sistemática por parte de los administradores de la red.

La preocupación del mercado está en desarrollar herramientas informáticas que permitan de una u otra forma darle solución al problema de la seguridad informática, se sabe que en el mercado existen múltiples productos que utilizan gestión remota, productos que buscan filtrar la penetración de extraños nuestra intranet, productos que buscan la eliminación de virus, productos que buscan luchar contra programas espías, productos

que buscan controlar políticas de seguridad informáticas, productos que buscan controlar el acceso a sitios web, productos que buscan controlar el uso de aplicaciones concretas en Internet como por ejemplo Chat, productos que buscan controlar la instalación de software no autorizados por el administrador de red, productos de auditoria informática, productos educativos, pero debido a que no es rentable para la empresa privada no se ha creado un producto que integre o trate de integrar por medio de políticas las principales características de estos productos en uno solo. Veremos varios productos que agrupan de una u otra forma algunas características comunes a Hegcon-PS.

1.1.2. Ejemplo de Productos Desarrollados en el Mercado:

_____

1.1.2.1. INTERNET – POLICY. **http://www.internet-policy.com/services_es.html**

Internet-Policy permite a las organizaciones el desarrollo y puesta en práctica de políticas coherentes y reales para el acceso y uso de Internet y el correo electrónico por parte de usuarios internos y externos.

A esto hay que añadir que Internet Policy ayuda a asegurar que una política online bien definida es apoyada y soportada por soluciones técnicas efectivas.

Auditor : Internet Policy se enfoca en primer lugar en la realización de una auditoria, que evalúa las fortalezas y debilidades de la política y prácticas de la organización en relación al uso de Internet por parte de sus empleados y con sus clientes.

1.1.2.2. Consul/Eaudit.

http://www.consul.com/files_download/demo/Ceademoguide.pdf

Consul/Eaudit es otra herramienta software para seguridad informática que aumenta el nivel de seguridad de una empresa generando una conducta de confianza al penetrar al mundo de la Internet, esta herramienta permite la reducción de costos en la dirección de la red. Consul/eAudit permanentemente está realizando el monitoreo en toda la red y realiza el control de las políticas de seguridad en una empresa, registra todos los acontecimientos además que supervisa automáticamente el entorno descentralizado. Los datos de registro a través del ambiente de plataformas, se recogen automáticamente y se consolida en una base de datos centralizada. Los registros se estandarizan en un lenguaje común y se comparan con las políticas de seguridad activas. Consul/eAudit realiza intervenciones automáticas, entrega las excepciones, faltas y las atenciones basadas en las políticas de seguridad, de la misma manera que lo realizaría un interventor humano.

Todas las excepciones a las políticas de seguridad emergen inmediatamente, en un informe común, claro y comprensible, no importa dónde se origino el acontecimiento. Consul/eAudit recoge los registros de seguridad de diversas plataformas y las archiva en un server.Audits centralizado, este procedimiento se realiza automáticamente. Los acontecimientos se basan en las políticas de seguridad establecidas.

1.1.3. Sistema Hegcon-PS

El sistema Hegcon-PS es una herramienta de gestión y control de políticas de seguridad computacional, el cual permite automatizar la planificación, dirección y el cumplimiento de las políticas de seguridad informática de una organización, con ahorros significativos en tiempo y dinero ya que elimina las actividades repetitivas y redundantes asociadas con estas tareas, evitando así los errores humanos que comúnmente aparecen al delegar las mismas a empleados de la organización.

Hegcon-PS cuenta con un lenguaje de políticas de seguridad desarrollado para implementar mediante políticas las diferentes características que ofrecen muchos productos en el mercado, con Hegcon-PS las políticas son creada por el administrador e implementadas de inmediato ya que se cuenta con un lenguaje de políticas de seguridad sencillo de utilizar en el gestor, este producto posee unos agentes quienes son unos representantes del esquema de seguridad en cada equipo, los agentes poseen un interprete del lenguaje de políticas de seguridad, los cuales toman la información enviada por el gestor de forma remota y esta en la capacidad de asignar tareas en el sistema permitiendo se cumplan e implementen remotamente las políticas creadas en el gestor.

Es de anotar que esta es una herramienta muy útil, ya que todo los procesos que se puedan llevar acabo en un terminal lo podemos lograr mediante instrucciones, solo hace falta conocimiento del lenguaje de políticas de seguridad para sacar de esta herramienta su mejor provecho, en primera instancia se presenta esta herramienta como educativa, pero en la 2ª versión estará en la posibilidad de ser educativa y restrictiva, además de estos se implementaran políticas multiplataformas.

El sistema Hegcon-PS está enfocado a un proceso educativo para los usuarios de la red de la Universidad del Cauca, proceso en el cual aprenderán las medidas mínimas de seguridad que deben tener en cuenta para proteger la red y por lo tanto la información existente en cada computador. Hegcon-PS cuenta con interfaces visuales amigables y llamativas, en las cuales se les muestra a los usuarios los distintos mensajes educativos a medida que estos mismos infrinjan cada una de las políticas de seguridad implementadas en la red de la Universidad del Cauca.

El sistema Hegcon-PS proporciona medios eficaces de administrar y controlar la política mientras suministra informes que permiten demostrar en forma concluyente los avances en la implantación de esta política desde la propia estación de trabajo del administrador de seguridad a cargo. Es un sistema que se implemento utilizando la plataforma Windows 98, ya que es el software licenciado actualmente por la Universidad del Cauca.

El sistema Hegcon-PS se desarrollo basados en la arquitectura del Gestor / Agente permite definir dominios con perfiles de sistemas de seguridad similares.

Para iniciar un proceso de verificación el gestor informa a cada agente que realice la comprobación de seguridad especificada, una vez está completada, el agente envía los datos resultantes al gestor.

Sólo se transmiten datos que son absolutamente requeridos, esta es una inmensa ventaja sobre otros productos que constantemente sondean[4] los sistemas a través de la red para conseguir información de seguridad.

Simplemente se inicia una comprobación de seguridad desde la interfaz gráfica del sistema Hegcon-PS para obtener un estado detallado de todos los sistemas que conforman su red corporativa, corrigiendo los estados de seguridad con problemas, muchas veces en línea desde la propia interfaz gráfica.

1.2. Funcionalidad del Sistema Hegcon-PS

Hegcon-PS identifica violaciones a las políticas establecidas, despliega esta información de una manera gráfica que hace mucho más fácil la detección de problemas de manera instantánea.

Las políticas pueden ser específicas a los estándares de seguridad, pueden ser universales para todos los grupos y todos los sistemas.

Una vez que las políticas son definidas por el gestor[5], Hegcon-PS realiza un monitoreo constante de cada grupo o cada sistema para asegurar su conformidad con la política

[4] Sondean: Hacer preguntas para averiguar la intención de uno o las circunstancias de algo:

establecida. Hegcon-PS analiza estos datos y despliega gráficamente la información en detalle o en resumen sobre cualquier área donde la política de seguridad no se respeta. Si Hegcon-PS identifica un problema, éste puede notificar al usuario sobre la violación de la política y enviaría al gestor un reporte, donde se detalla el nombre del usuario, la dirección IP, la hora y la dirección MAC del equipo donde se están violando las políticas.

1.3. Ambiente de Desarrollo del Sistema Hegcon-PS

Este proyecto se realizó en los laboratorios de informática de la Universidad del Cauca, utilizando como prototipo de pruebas 5 políticas de seguridad que se estudiaron por un comité que se integro por personal de la red de datos y personal del grupo de investigación de seguridad computacional de la Universidad del Cauca, los cuales dieron viabilidad a la implementación de estas políticas, estas son: Control de Instalación del Agentes, Control de Software no autorizado por el administrador, Control de visitas a sitios no autorizados por el administrador, Control de mecanismos de protección contra virus informáticos, Control de recursos compartidos.

Es de anotar que en la red de la Universidad del Cauca no se cuenta con políticas de seguridad computacional implementadas. No se cuenta en la universidad con un proceso continuo de enseñanza a cerca de las medidas de prevención que se deben tener para utilizar los equipos y conectarse a Internet.

Es por esta razón que continuamente la universidad invierte dinero en el pago de técnicos para que se desplacen a los puntos donde se han presentado problemas de des-configuración o pérdida de información causados por virus. Es de anotar que en la actualidad se cuenta con un servidor de antivirus el cual protege a la universidad de

[5] El Gestor. Corresponde a una Aplicación Software de mayor jerarquía instalado en la posición del Servidor mediante el cual el Administrador de red puede gestionar las políticas de seguridad que se desean controlar por medio de los Agentes de Control.

ataques externos, pero no hay control sobre los ataques provenientes del interior de la universidad.

Una parte muy importante y de mucho cuidado es que la universidad se encuentra en riesgo por la instalación de software sin licencia por parte de los usuarios al interior de la universidad sin la debida autorización.

Esto traería inconvenientes una vez seamos visitados por las autoridades reguladoras de derechos de autor (Fedesoft)[6]. Una vez verificada estas anomalías por parte de las autoridades pertinentes, la universidad se vería en problemas legales teniendo que pagar multas muy altas debidas a esta falla en el control de una política de seguridad (ver tabla1 Resumen del valor riesgo anual en la Universidad del Cauca por falta de control de políticas).

Esta herramienta esta en la capacidad de controlar tales anomalías por medio de un método de verificación de software, en donde desde el gestor se crea la lista del software permitido y licenciado por parte de la universidad, por tanto el sistema catalogara como una violación de política la utilización o instalación de software no autorizado, de esta forma al usuario se le desplegara un mensaje informándolo sobre la violación a la política de control software y a la vez le envía un reporte al gestor.

[6] Fedesoft: Federación Colombiana de la Industria de Software y Tecnologías Informáticas Relacionadas. Defiende los intereses sectoriales de la Industria de Software y Tecnologías Informáticas Relacionadas en Colombia. www.fedesoft.org.

Tabla 1. Resumen del valor riesgo anual en la Universidad del Cauca por falta de control de políticas.
Fuente: Ing. Maria Clara Rodríguez. Jefe División de Sistemas

Concepto del Gasto	Valor
Alteración y daños de los sistemas de computo(causados por virus, recursos compartidos y programas malignos: Se tienen en cuenta para este presupuesto el 50% del personal disponible para solucionar estas tareas diariamente).	$259´200.000
Alteración y daños de la información causada por virus, carpetas compartidas o mal manejo de los recursos computacionales. (Tiempo perdido en la generación de la información, tiempo intentando la recuperación de la misma y el tiempo gastado en la nueva construcción de la información cuando hay pérdida total de la misma. Sin considerar los costos generados cuando la información es robada o los equipos son decomisados por software pirata).	$185´000.000
Multa a las que se debería enfrentar la universidad por falta de licencias por software pirata, decomiso de equipos y pérdida de la información.(En la actualidad la universidad no cuenta con licencia de productos Microsoft y se considero para este presupuesto solo la sancion con el 50% de los equipos existentes en la universidad, teniendo en cuenta que existen aproximadamente 100 tipos distintos de software sin licencia "piratas" instalados en equipos de la universidad)	$1.850´000.000
Robo o cambio de dispositivos de los equipos de cómputo (Se presenta diariamente los robos y cambios de discos duros, memorias, correas y otros dispositivos informaticos) .	$ 45´000.000
Total valor de riesgo anual	$2.339´200.000

1.4. Propósitos Principales del Proyecto

Desarrollar una aplicación distribuida para gestionar y controlar políticas de seguridad, buscando sea implementada en la red de datos de la Universidad del Cauca, de esta forma se incremente el nivel de seguridad de los servicios que la red ofrece actualmente, se pretende crear una nueva cultura, educando a los usuarios para la utilización optima de los sistemas, recursos y servicios de red. Esta aplicación estará en la capacidad de llevar a cabo los siguientes procesos:

- Capturar información del registro de actividades del usuario
- Auditar[7] las actividades del usuario de acuerdo a las políticas implementadas en el gestor.
- Educar a los usuarios sobre el uso correcto de los recursos y servicios de red de acuerdo a las políticas implementadas en el gestor.
- Auditar las configuraciones del sistema de archivo y del registro de configuraciones con el fin de detectar vulnerabilidades en el sistema.
- Implementar mecanismos de protección contra virus informáticos.
- Control adecuado del uso de los recursos compartidos.
- Llevar acabo el control de acceso a sitios no autorizados detallados en la política creada por el gestor.
- Controlar la instalación de software no autorizado por la administración de la red.

[7] Auditar: inspeccionar las condiciones en que se encuentran las cosas o como se llevan acabo procedimientos.

2. FUNDAMENTOS DE SEGURIDAD EN REDES INFORMATICAS

En este capítulo se desarrollaran los conceptos generales de seguridad informática en redes computacionales, así como los riesgos y amenazas a los cuales está expuesta una red de comunicaciones informáticas. De esta forma se generarán las bases de conocimiento suficiente para entender de forma precisa las causas que conllevan al desarrollo de este proyecto.

2.1. La Seguridad Informática.

Cuando se habla de seguridad informática se entiende como algo tan grande y complicado que se cree que no les atañe a los simples usuarios no les atañe. Es cierto que la temática es complicada y profunda, pero si cada persona como simple usuario de la Internet no toma las medidas cautelares y preventivas de seguridad informática, o violan los procesos de seguridad sugeridos por los administradores de red, de forma indirecta se están convirtiendo en cómplices del atacante, ya que en este momento han abierto la puerta y no han tenido el cuidado de cerrarla, por esta razón los han robado y han hecho daño en sus propios equipos (Intranet)[8]. El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en forma antes imposible de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en forma no tradicionales.

La mayoría del mundo informático desconoce la magnitud del problema con el que se esta enfrentando y es por esta razón que no se invierte en capital humano ni tecnológico

[8] Intranet: Red de área local

necesario para prevenir principalmente el daño y/o perdida de la información que en última instancia es la herramienta de trabajo.

Así como el estado Colombiano posee una constitución provista de leyes para la seguridad y protección de cada uno de sus ciudadanos, de igual forma las entidades empresariales o educativas deben contar con reglas, normas y políticas de seguridad informática que permitan la protección de sus computadoras y de la información existente en cada uno de estas.

Desde el punto de vista técnico, la seguridad se encuentra en las manos de los dirigentes de las organizaciones, y en última instancia en cada uno de los usuarios. Una vez implementados los mecanismos de seguridad en una organización, esta depende del grado de concientización respecto a la importancia del problema y de que tanto les interesa la protección de la información y el sostenimiento de la organización.

En el presente cada vez que se mencione la palabra información se estará haciendo referencia a la información que es procesada por un sistema informático; definiendo este ultimo como el "Conjunto formado por las personas, computadoras (Hardware y Software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones". Luego, "El objetivo de la seguridad informática será la protección de la integridad, la disponibilidad, autenticidad y privacidad de la información por medio de la implementación de políticas de seguridad"[2] .

Podemos definir varios aspectos que involucra la seguridad informática, como son:

- Seguridad física
- Seguridad lógica

2.2. Seguridad Física

Se abarca de forma conjunta la seguridad física y seguridad locativa. La seguridad locativa consiste básicamente en las precauciones que se deben tomar para proteger el acceso y la integridad del lugar donde se encuentran ubicados los equipos de cómputo y se encuentra estrechamente ligada con las protecciones de tipo físico que se deben implementar.

La seguridad física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[2] . Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo implementados para proteger el hardware y medios de almacenamiento de datos.

La exposición a riesgos físicos y ambientales puede producir pérdidas financieras, repercusiones legales, pérdida de credibilidad o pérdida de competitividad. Las áreas que deben protegerse son las siguientes:

- Área de Programación.
- Sala de la computadora principal.
- Consolas y terminales del operador.
- Biblioteca de los medios magnéticos de almacenamiento.
- Área de almacenamiento de las reservas fuera de los predios de la institución.
- Sala de control de entrada y salida.
- Cuarto de conexiones de comunicaciones.
- Equipo de telecomunicaciones (radios, satélites, cableado, módems, etc.).
- Microcomputadoras y computadoras personales.
- Fuente de energía eléctrica.
- Líneas telefónicas dedicadas.
- Equipo portátil (scanner, lectores de código de barras, impresoras, y otros).

- Impresoras en ubicaciones locales o remotas.
- Redes de comunicaciones.

El acceso físico a las áreas mencionadas sólo se le permitirá al personal autorizado por la gerencia o administración de la red. Todas las personas que requieran acceso a las áreas indicadas lo harán bajo un control adecuado y acompañados del supervisor o funcionario autorizado del área de operación.

La seguridad física de los sistemas de información computadorizados requiere disponer de procedimientos y medidas que contrarresten los riesgos a los daños que puedan causar el fuego, el agua, las interrupciones o variaciones de la energía eléctrica que alimenta a los equipos, así como por la presencia de químicos y otros elementos que afecten el ambiente normal de operación de las máquinas y del estado físico de los archivos magnéticos.

En atención a lo anterior, deberá disponerse de dispositivos de detección de fuego y humedad, así como de extintores de fuego apropiados (manuales y sistemas de supresión de incendio), alarmas de incendio y detectores de humo, los cuales deberán ser inspeccionados y probados periódicamente para asegurar su uso en el momento requerido. También deben ofrecer el adiestramiento necesario al personal que garantice su adecuada utilización.

Características de construcción: los edificios o instalaciones de una empresa donde estén, o vayan a estar, situados sus sistemas de información requieren unas características adicionales de protección física que deben ser consideradas antes de seleccionar su ubicación, teniendo en cuenta:

- La posibilidad de daños por fuego, inundación, explosión, disturbios civiles, amenazas de vecindad, cercanía de instalaciones peligrosas (depósitos de combustible, aeropuertos, acuartelamientos, etc.).
- Cualquier otra forma de desastre natural o provocado. Adicionalmente,

- Estas instalaciones deben estar diseñadas de forma que no se faciliten indicaciones de su propósito ni se pueda identificar la localización de los Recursos informáticos.
- Deben incluir zonas destinadas a carga y descarga de suministros, y su inspección de seguridad. Si todos los materiales no pueden ser inspeccionados en el momento, debe habilitarse una zona de consigna o depósito de materiales transeúntes hasta que puedan ser revisados.
- Tienen que disponer de canalizaciones adecuadas para la conducción del cableado de comunicaciones y electricidad, para evitar ataques (sabotaje, fuego, roedores), interceptación o perturbaciones por fuentes de emisión próximas (radio, eléctricas, calor, etc.).

Por otra parte se debe hacer una correcta distribución de las áreas y la forma como deben de ser controladas las edificaciones donde funcionara el sistema de cómputo.

2.3. Seguridad Lógica

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo"[2] . Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido"[2] y esto es lo que debe asegurar la Seguridad Lógica. Los objetivos que se pretenden alcanzar por parte de los administradores de red al momento de implementar políticas de seguridad son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas autorizados al usuario.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no por otro.

- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que diariamente se haga un backup de la información de la compañía y se guarde en un lugar seguro.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Para evitar accesos no autorizados se pueden implementar los controles de acceso, los cuales constituyen una importante ayuda para proteger a todo el sistema de la mala utilización o modificaciones no autorizadas, de esta forma podemos tratar de mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido), resguardando también la información confidencial de accesos no permitidos.

Se deben implementar la identificación y autenticación, la cual constituye la principal defensa para la mayoría de los sistemas computarizados, evitando el ingreso de personal no autorizado. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se puede controlar el acceso a la información a través de roles de usuario, es decir el programador tiene acceso solo a la información que le compete, el director tiene acceso a la información que le corresponde manejar, el gerente a su información, de esta manera cada uno tiene acceso solo a la información que le corresponde.

Al momento de transmitir información podemos utilizar métodos de encripción asimétricos utilizando llaves públicas y privadas, lo cual de cierta forma garantiza que la información solo puede ser leída por el destinatario final, el cual posee la llave publica del usuario que la envió.

2.4. Objetivos de la Seguridad Informática

La Seguridad Informática se define, como la estructura de control establecida para gestionar la disponibilidad, integridad, confidencialidad y consistencia de los datos, sistemas de información y recursos informáticos[8] .

La seguridad persigue tres objetivos básicos:

Confidencialidad: Con esta se busca:

- Proteger la revelación de información a personas no autorizadas
- Restringir el acceso a información confidencial
- Proteger el sistema contra usuarios curiosos internos y externos

Por confidencialidad se entiende el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. En áreas de seguridad gubernamentales la confidencialidad asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas.

En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la

defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son: El uso de técnicas de control de acceso a los sistemas. El cifrado de la información confidencial o de las comunicaciones.

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

Con la integridad se busca:

- Proteger los datos de cambios no autorizados
- Restringir la manipulación de datos a programas autorizados
- Proveer información verídica y consistente

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseada la información. Por ejemplo, que los datos recibidos o recuperados sean exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados. En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad.

Con la autenticidad se busca proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos. En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad).

En el campo de la criptografía hay diversos métodos para mantener y asegurar la autenticidad de los mensajes con la precisión de los datos recibidos. Se usan para ello códigos, firmas añadidas a los mensajes en origen y recalculadas y comprobadas en el destino. Tenemos como ejemplo el método autenticidad, este método puede asegurar no sólo la integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de los mismos (quién lo envía es quien dice que es).

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

Con la disponibilidad se busca:

- Asegurar la continuidad operativa del sistema y proveer planes alternativos de contingencia.
- Proteger el sistema contra acciones o accidentes que detengan los servicios o destruyan la información que brinda.

La situación que se produce cuando se puede acceder a un sistema informático en un periodo de tiempo considerado aceptable. Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio"[9]. El computador puede estar dañado o haber una caída del sistema operativo. No hay suficiente memoria para ejecutar los programas, los discos, cintas o impresoras no están disponibles o están llenos. No se puede acceder a la información. De hecho, muchos ataques, como el caso de los virus

[9] "Denegación de servicio" : Significa que los usuarios no pueden obtener del sistema los recursos deseados.

Works, buscan también bloquear el sistema o retrasar la red creando nuevos procesos que saturaban recursos.

Autenticidad: Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro, Imposibilidad de rechazo (no-repudio). Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió. Esta propiedad y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

2.5 Riesgos y Amenazas

La amenaza más reciente a los recursos de computo y la información pudiera parecer únicamente los virus computacionales, sin embargo existen otro tipo de amenazas a la seguridad de los recursos informáticos como son:
Sabotaje, robo de información, espionaje, daño total o parcial de sus recursos e información por catástrofes naturales, terremotos, tormentas, actos terroristas, inundaciones, incendios, etc., estos son solo algunos de los riesgos a los cuales nos podemos ver enfrentados.

Pero lo más importante es contar con un plan de contingencia en caso de desastres, políticas de seguridad de los recursos informáticos que nos permitan controlar fallas internas, además de eso tener a la mano un análisis y evaluación de riesgos informáticos que pueda sufrir nuestro información. Contar con un sistema de respaldo periódico de nuestra información y un lugar de almacenamiento alternativo de esos respaldos, ya que estos pueden ser dañados por distintos tipos de virus que se describen a continuación.

2.5.1 Virus Informáticos

Los virus informáticos son uno de los principales riesgos de seguridad para los sistemas, ya sea que estemos hablando de un usuario hogareño que utiliza su máquina para trabajar y conectarse a Internet o una empresa con un sistema informático importante que debe mantener bajo constante vigilancia para evitar pérdidas causadas por los virus.
Un virus se valdrá de cualquier técnica conocida o poco conocida para lograr su cometido. Encontraremos virus muy simples que sólo se dedican a presentar mensajes en pantalla y otros mucho más complejos que intentan ocultar su presencia y atacar en el momento justo.

Se dará una visión general de los tipos de virus existentes para poder enfocarnos más en cómo proteger un sistema informático de estos atacantes y cómo erradicarlos una vez que han lograron penetrar.

Definición de virus informático: "Un virus informático es un pequeño programa, invisible para el usuario (no detectable con el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye la información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismo (completas, en forma discreta, en un archivo, disco u computador distinto al que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas afectados e información y/o hardware (en forma lógica)". **[9]**

Aparentemente el primero en acuñar el término virus en informática, fue el Dr Fred Cohen en 1985 resaltando la particularidad más relevante del mismo y que compartía con su contraparte biológica: La capacidad de auto reproducción. Esta característica, junto a la capacidad de permanecer general mente oculto o invisible al sistema operativo (y por tanto al operador), son las que diferencian a un virus de otros programas destructivos y

cualquier definición que no las incluya sólo estará refiriéndose a la generalidad de tales programas.

Un virus tiene tres características primarias:

- **Es dañino.** Un virus informático siempre causa daños en el sistema que infecta, pero vale aclarar que el hacer daño no significa que valla a romper algo. El daño puede ser implícito cuando lo que se busca es destruir o alterar información o pueden ser situaciones con efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador, etc.
- **Es auto reproductor**. La característica más importante de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace. Imagínense que si todos tuvieran esta capacidad podríamos instalar un procesador de textos y un par de días más tarde tendríamos tres de ellos o más. Consideramos ésta como una característica propia de virus porque los programas convencionales pueden causar daño, aunque sea accidental, sobrescribiendo algunas librerías y pueden estar ocultos a la vista del usuario, por ejemplo: un programita que se encargue de legitimar las copias de software que se instalan.
- **Es subrepticio**. Esto significa que utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia. La primera medida es tener un tamaño reducido para poder disimularse a primera vista. Puede llegar a manipular el resultado de una petición al sistema operativo de mostrar el tamaño del archivo e incluso todos sus atributos.

La verdadera peligrosidad de un virus no está dada por su arsenal de instrucciones maléficas, sino por lo crítico del sistema que está infectando.

Los virus informáticos no pueden causar un daño directo sobre el hardware. No existen instrucciones que derritan la unidad de disco rígido o que hagan estallar el cañón de un monitor. En su defecto, un virus puede hacer ejecutar operaciones que reduzcan la vida útil de los dispositivos. Por ejemplo: hacer que la placa de sonido envíe señales de

frecuencias variadas con un volumen muy alto para averiar los parlantes, hacer que la impresora desplace el cabezal de un lado a otro o que lo golpee contra uno de los lados, hacer que las unidades de almacenamiento muevan a gran velocidad las cabezas de L / E para que se desgasten. Todo este tipo de cosas son posibles aunque muy poco probables y por lo general los virus prefieren atacar los archivos y no meterse con la parte física.

Clasificación de virus: Dependiendo del lugar donde se alojan, la técnica de replicación o la plataforma en la cual trabajan, podemos diferenciar en distintos tipos de virus. **[2]**

- Virus de sector de arranque
- Virus de archivo
- Virus de macro
- Virus bat
- Virus del mirc
- Virus polimorficos
- Virus stealth
- Virus multipartitos

Cada uno de estos virus tienen distintos formas de infección, y distintas formas de contrarrestarlos con antivirus (Ver **anexo A**).

Amenazas externas: Las amenazas que se ciernen sobre los sistemas informáticos tienen orígenes diversos. En este caso consideraremos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, terremotos, sabotajes, y otros. Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos inmensos y frecuentemente por errores de operación, además de esto las líneas de comunicación pueden ser interferidas o “pinchadas “, etc.

Emergencia y evacuación: Tiene que haber implantado, de acuerdo con las Leyes y reglamentos en vigor, especialmente con la Norma NBE/CPI-91[10] un Plan de Emergencia y Evacuación de las instalaciones de la empresa.

Los objetivos de este Plan deben ser conocer los edificios y sus instalaciones, las áreas de posibles riesgos y los medios de protección disponibles;

- Evitar, o al menos minimizar, las causas de las emergencias;
- Garantizar la fiabilidad de los medios de protección;
- Tener informados de las medidas de protección a todos los ocupantes de las instalaciones;
- Disponer de personal organizado y adiestrado para las situaciones de emergencia;
- Hacer cumplir la vigente normativa de seguridad;
- Preparar la posible intervención de recursos externos (Policía, Bomberos, Ambulancias, etc.).

Hay que subrayar que la responsabilidad de confeccionar y mantener actualizado el plan recae en una función ajena a sistemas de Información. No obstante, es necesaria su colaboración en el desarrollo de las medidas a tomar, relacionadas con las instalaciones informáticas, sus operaciones y las personas que trabajen en ellas.

Sistemas de detección: Las áreas Controladas deben contar con medios de detección de situaciones anómalas y previsibles para el área, tales como: puertas abiertas, acceso de intrusos, inundación, incendio o humos, etc.

[10] NBE-CPI/91, Norma básica de la edificación. Condiciones de protección contra incendios en edificios comerciales. Aprobada por el Real Decreto 279/1991 del parlamento Europeo de 1 de marzo, y, en su caso, al anexo C «Condiciones particulares para el uso comercial», aprobado por el Real Decreto 1230/1993, de 23 de julio;

Su objetivo es permitir un conocimiento inmediato y preciso del hecho y su localización, por lo que su actuación debe ser absolutamente fiable dentro de unos parámetros previamente establecidos. Ello exige unas revisiones de funcionamiento y un riguroso mantenimiento preventivo cuya periodicidad dependerá del sistema de detección y del tipo de área Controlada al que se aplique.

La detección de un hecho anómalo requiere la información necesaria para una reacción proporcionada. Dependiendo de la información suministrada por el medio de detección y de los parámetros previamente establecidos, antes de llegar a un estado de Alarma se puede pasar por un estado de Alerta, en el que algunos medios de reacción se van armando en previsión de su posible actuación.

Todos los medios de detección pueden integrarse en un único sistema, preferentemente automático, que los gestione y que:

- Avise de la anomalía y su gravedad;
- Inicie acciones de corrección automáticas
- Proponga acciones manuales a realizar por personal entrenado para ello;
- Controle las actuaciones (qué, quién, cómo, dónde y cuándo).

Este sistema debe estar bajo vigilancia permanente y combinado con los servicios de mantenimiento, para los casos de mal funcionamiento de cualquier medio de detección.

Hay que subrayar que los sistemas de Detección deben funcionar incluso con el suministro eléctrico de emergencia.

Sistemas de Extinción de Incendios: En caso de incendio, su extinción puede realizarse con medios manuales o automáticos.

Los medios manuales se basan en extintores portátiles, mangueras, etc. Es importante resaltar que el elemento extintor localizado en un área debe ser el apropiado para el

previsible tipo de incendio a declararse en ella. Cualquier medio de extinción puede ser excelente, utilizado en un área o más dañino que el propio fuego, si es usado en otra. Nunca debe emplearse un medio de extinción manual basado en agua donde pueda haber fuego eléctrico, por peligro de electrocución. No es aconsejable la intervención de personal no entrenado para ello. Siempre que se disponga de tiempo, hay que avisar a la Brigada Interior de Incendios (si la hubiera) o al Servicio de Bomberos.

Los medios automáticos se basan en la inundación del área mediante agua, CO2 o compuestos halogenados.

- El más recomendable es el basado en el agua, por su bajo coste y su nulo impacto en el entorno.

Los sistemas automáticos de extinción basados en el agua, deben tener un mecanismo de reacción que, en caso de llegar a un estado de Alerta o de Alarma, sustituye el aire de la conducción por agua. La actuación de estos sistemas de extinción debe estar combinada con la previa desconexión del suministro de energía eléctrica del área afectada.

Las áreas Controladas deben contar con medios automáticos y manuales de extinción de incendios.

3. POLITICAS INFORMATICAS: CONCEPTOS Y ESTRUCTURA

3.1 Definición de Política de Seguridad

Las fallas más grandes son las humanas, y en cuestiones de Seguridad Informática ésto es totalmente evidente. La organización y cada uno de sus integrantes (Administradores, monitores, auxiliares, usuarios, etc) son los responsables de llevar a su sistema de Información al mejor desempeño, lo cual implica instalaciones y configuraciones correctas de equipos, dispositivos, protocolos y conexiones. Sin embargo también implica un componente intangible pero vital, y en la mayoría de los casos ignorado; el planteamiento de directivas controlables sobre el correcto uso de los sistemas, recursos y servicios de red. Mientras esta etapa no se cumpla, cualquier red poderosa es muy vulnerable[11], lo cual afecta de lleno el valor del capital más importante de cualquier organización: LA INFORMACIÓN.

Una Política de Seguridad se define como la especificación de los requerimientos para el control de acceso a la información, aplicaciones y servicios de una organización.

Dentro de las funciones de las entidades informáticas, las políticas de seguridad se deben enfocar inicialmente a la protección de la información almacenada, procesada y distribuida mediante sus recursos; sin embargo, también se deben emitir políticas para todos los rubros, incluyendo facilidades, aplicaciones, instalaciones y equipos.

Una buena política de seguridad deja poco campo a la interpretación. Es muy importante que los usuarios y todos los que intenten usar un computador de la red para acceder a sus servicios conozcan y entiendan las reglas del sistema.

[11] "vulnerable": Que puede ser atacado o dañado.

3.2. Importancia de las Políticas de Seguridad

Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de la entidad. Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos. Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos.

Sobre todo es importante que la organización defina claramente y valore que tan importantes son los recursos e información que se tienen en la red corporativa y dependiendo de esto, justificar si es necesario que se preste la atención y esfuerzos suficientes para lograr un nivel adecuado de protección. La mayoría de las organizaciones poseen información sensible y secretos importantes en sus redes, esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos como propiedades de la corporación y edificios de oficinas.

Una política de seguridad en un sitio es requerida para establecer a lo largo de la organización un programa de como usuarios internos y externos interactúan con la red de computadores de la empresa.
Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y cuando la política no disminuya

la capacidad de la organización, es decir la política de seguridad debe ser de tal forma que no evite que los usuarios cumplan con su tarea en forma efectiva

Para lograr un efectivo control sobre todos los componentes que conforman la red y asegurar que su conectividad[12] a otras redes no es algo fácil, es necesario primero que todo establecer con exactitud que recursos de la red y servicios desea proteger, de tal manera que este preparado para conectar su red con el resto del mundo. Esto implica el estudio y definición de los aspectos necesarios para la planeación de la seguridad de la red, análisis de riesgos, identificación de recursos y amenazas, uso de la red y responsabilidades, planes de acción o contingencia, etc.

3.3. Creación de Políticas de Seguridad Informática

Crear políticas es, por definición, especificar las necesidades de control de acceso a la información. En particular, las políticas deberán reflejar los objetivos de la Institución con respecto a la relativa importancia de cada rubro a proteger y la manera en que esa información contribuye a la misión de cada Institución. Por su parte, las normas, procedimientos, prácticas y estándares, deberán acoplar esas necesidades con los recursos técnicos existentes en la Institución e incidirán en su caso en la modernización de los esquemas técnicos de seguridad.

Una manera formal de iniciar la generación de políticas, es el atacar tópicos básicos con fundamento en aspectos generales, aplicables al entorno de responsabilidad de todas las Instituciones. Este paso deberá enriquecerse con aspectos específicos a cada entorno en particular.

Cuando se habla de un documento de Políticas de Seguridad, no se trata de un documento general, ya que por definición debe responder a las necesidades y características de la Institución que incorpora las políticas; se refiere a un documento dinámico, es decir, que requiere de constante revisión para mantenerlo vigente, no por

[12] "Conectividad": Cualidad de lo que es conectivo: conectividad de las comunicaciones.

exaltarlo o por ocio, sino por cuestiones de legítima seguridad, sobre todo en ámbitos tan cambiantes como lo es la Internet, donde la vigencia de las soluciones técnicas y administrativas es de primordial importancia para mantener nuestros sistemas confiables.

3.4. Estructura de las Políticas de Seguridad

Dependiendo de la amplitud de las situaciones que pretenda abarcar una política, la misma puede ser clasificada en los siguientes niveles jerárquicos como se describe en la tabla 2.

Tabla 2. Clasificación de una política de seguridad

Niveles de Políticas:	Objetivo:
Política general	Visión de seguridad respecto a todo el servicio de Internet.
Política específica a un tema	Se orienta a tópicos que tienen un interés específico
Política particular a una aplicación	Se enfoca a decisiones tomadas por la administración para proteger aplicaciones o sistemas particulares

Partiendo de las políticas generales, el grado de detalle y complejidad requerido aumenta conforme se avanza hacia las políticas particulares. Así mismo, entre más detallada y compleja es una política, se requiere actualizarla más frecuentemente y es más complicado el proceso de implantación de la misma.

Por otro lado, de acuerdo al recurso al que está dirigida una política, ésta puede ser clasificada en varios tipos básicos como se muestra en la tabla 3.

Tabla 3. Clasificación de la política informática de acuerdo al recurso dirigido

Recursos:	Objetivo:
Orientada a los recursos lógicos.	Cuando el recurso tiene que ver con las técnicas empleadas para generar, explotar o intercomunicar tanto aplicaciones como los datos asociados a las mismas.
Orientada a la recursos de gestión	Cuando el recurso tiene que ver con aspectos administrativos, de personal o con la misma estructura organizacional de la Dependencia
Orientada a los recursos físicos	Cuando se trate de bienes materiales como instalaciones y equipos
Orientada a la respuesta ante incidentes	Cuando se trate de los recursos empleados durante y después de una contingencia.

3.4.1. Estructura Jerárquica de las Políticas de Seguridad en la Información

Identificar la ubicación jerárquica de las Políticas de Seguridad dentro de la dependencia, permite por un lado, hacia arriba, mantener la congruencia con los objetivos institucionales, y por otro, hacia abajo, normar los procedimientos de operación en observancia a las Políticas de Seguridad definidas como se muestra en el Grafico 1.

Es evidente que entre más alto sea el nivel jerárquico de los enunciados regulatorios, las modificaciones serán mínimas, pero serán más generales y legislativa ente más robustos, mientras que los niveles inferiores estarán más apegados a soluciones muy concretas, por lo que su modificación puede ser más frecuente.

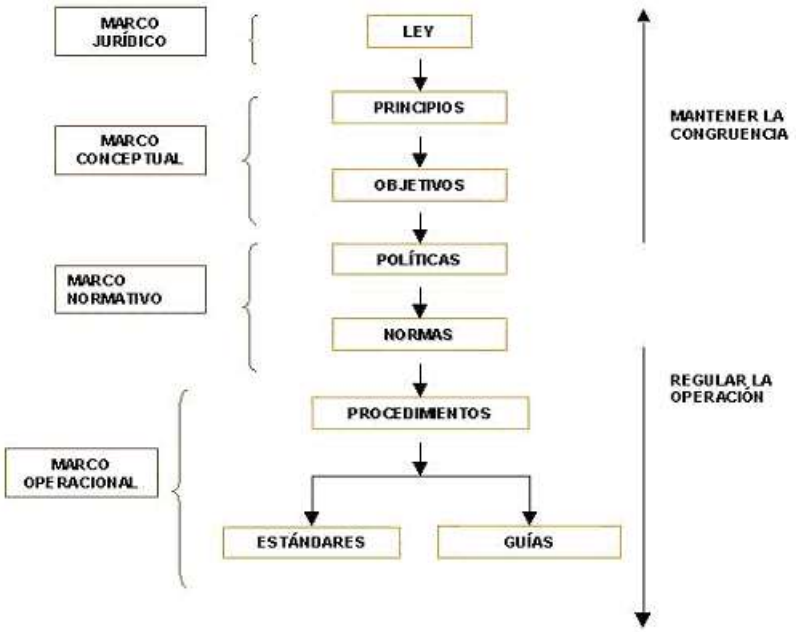

Figura 1. Estructura jerárquica de la seguridad en la información.[4]

3.4.2. Descripción de la Estructura:

Marco Jurídico.- Define la Ley o Leyes que dan origen a la creación por decreto de la Institución o Dependencia, la cual mantendrá su vigencia o espíritu mientras encuentre el sustento jurídico que permite su existencia.

Ley.- Sustenta la existencia legítima de la Institución.

Marco Conceptual.- Es el espíritu institucional dentro del que se engloban los valores y metas de la Institución, en concordancia con la naturaleza de la ley que la origina.

Principios.- Esencia moral y ética de la Institución.

Objetivo.- Propósito de la Institución.

Marco Normativo.- Es el conjunto de preceptos que regulan la conducta institucional con el fin de llevar a buen término sus objetivos.

Políticas.- Forma en que se cumple con el objetivo

Normas.- Regla específica que debe cumplirse; su omisión causará la sanción respectiva.

Marco Operacional.- Es el conjunto de elementos de orden que definen la operación de los esquemas de manejo de información.

Procedimientos.- Son instrucciones precisas para el desarrollo de actividades.

Estándares.- Procedimientos apegados estrictamente a la norma.

Guías.- Procedimientos dirigidos u orientados, susceptibles de ser comentados o interpretados.

Como se observa, los procedimientos pueden ser estándares o guías; cuando sólo se recomienda la manera de hacer alguna tarea específica, se emite una guía, misma que no es obligatoria, sino una sugerencia de acción; por otro lado, un estándar es mucho más riguroso, y es de observancia obligatoria; cuando las guías son adoptadas y probadas en su efectividad, pueden pasar a ser estándares.

3.5. Descripción de las Políticas Piloto Implementadas.

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan cómo una organización maneja, protege y distribuye información sensitiva. Para efectos de implementación, el propósito es lograr que la gestión y control de políticas se haga de "forma dinámica"[13], por lo cual, el sistema Gestor-Agente proporciona una serie de argumentos y parámetros para facilitar al administrador de red el ensamblaje y gestión de las políticas que se desean controlar.

Esto también permitirá que las políticas no sean objetos estáticos y que se pueda modificar y mejorar su funcionamiento y rendimiento haciendo que el control de directivas de seguridad sea una labor adaptable a los distintos cambios en los mecanismos de protección de la Intranet[14]. Las políticas de seguridad de orden técnico que se han tomado como directivas piloto para implementar son:

> **Nota*:*** Este proyecto tiene un carácter totalmente educativo, y no es su intención generar directivas de tipo restrictivo que lleguen a atentar contra el libre uso de los recursos de Red por parte de los Usuarios ni generar polémicas en torno a asuntos sobre los cuales todavía no existe una reglamentación legal, penal y judicial que se puedan aceptar como parámetros de referencia. Por esto se aclara que en este proyecto se busca lograr una herramienta educativa que una vez implementada sirva como apoyo a la Administración de Redes Informáticas para llevar a los usuarios de red a hacer un muy buen uso de los recursos y servicios prestados por la red brindando de forma simultánea un nivel mas alto de seguridad a la organización.

[13] Forma dinámica: que las políticas no sean necesariamente permanentes y que se pueda modificar para mejorar su funcionamiento y rendimiento.
[14] intranet: Red de área local

3.5.1 Estructura de una Política de Seguridad

Riesgos

Una política de seguridad siempre debe constar de una etapa de análisis sobre el riesgo que se pretende erradicar o aminorar. Este análisis de riesgo se compone de los siguientes elementos:

- Evaluación económica de los impactos que puede generar la ausencia de un control de seguridad sobre los elementos críticos del sistema.

- Análisis de la probabilidad de que pueda ocurrir un evento que amenace la seguridad del sistema.

- Definición precisa del elemento o aspecto específico que se desea proteger mediante las directivas de seguridad.

A continuación se presentan algunos cuestionamientos que sirven como referencia para desarrollar la correspondiente evaluación de seguridad.

¿Qué fallas puede ocurrir en el comportamiento normal del sistema?
¿Con qué frecuencia puede ocurrir esta fallas?
¿Cuáles serían las consecuencias al darse dicha fallas?
¿Qué tan fiable es la información obtenida al responder las anteriores preguntas?
¿De qué manera está preparado el sistema para responder a dichas fallas?
¿Cuál es el costo de controlar dichas fallas?
¿Se tiene un control real sobre las operaciones del sistema?
¿Cómo responderá el sistema en el caso de que la seguridad haya sido violada?
¿Cuál información se considera confidencial o sensitiva dentro del sistema?
¿Está el sistema en capacidad de adecuarse a los cambios tecnológicos que puedan implicar una amenaza para su seguridad?

¿Qué usuario específico está autorizado para realizar operaciones sobre el sistema?

¿Cuáles son las responsabilidades y privilegios de cada uno de los distintos actores que componen el sistema?

Posterior a la evaluación anterior el sistema arrojará información que puede describirse en la tabla 4.

Tabla 4. Resultados de los análisis de riesgo [2].

tipoRiesgo	Valoración
RoboHardware	alto
RoboInformacion	alto
AtaquesIntrusion	medio
FallasSistema	medio
ProgramasMaliciosos	medio
EquivocacionesUsuario	medio
AccesoNoAutorizado	medio
FraudeLegal	medio
AmenazasFisicas	bajo

Amenazas

Existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe, la otra tampoco.

Las amenazas se pueden catalogar según el entorno en el cual operan.

Amenazas del entorno (que afectan la seguridad física)

Amenazas del sistema (que afectan la seguridad lógica)

Amenazas de la red (que afectan las comunicaciones)

Amenazas de personas (Insiders-Outsiders)

El alcance del proyecto **HEGCON-PS** se limita al desarrollo e implementación de políticas de seguridad que protegen el sistema de amenazas lógicas, y que pueden controlarse realizando operaciones sobre el sistema operativo de los equipos terminales.

3.6. Estrategias de Seguridad

Las estrategias pueden ser de dos tipos:
Proactiva[15]**.** se centra en reducir al mínimo los riesgos presentes en el sistema.
Reactiva[16]. se centra en una evaluación de consecuencias y daños a fin de realizar actividades de restauración del sistema y corrección de fallas.

Cuando se habla de seguridad informática se cumple literalmente

“Lo que no se permite expresamente está prohibido”

“Lo que no se prohíbe expresamente está permitido”

3.6.1. Implementación de la Política

Toda política que se quiera constituir en el gestor estará constituida los ítem que se describen en la tabla 5, los cuales corresponden la estructura de implementación con la cual se creo la aplicación Hegcon-PS y además servirán de referencia en la etapa de gestión de políticas.

[15] Pro-activa: A favor que las políticas implementadas fueran activas (restrictiva). (antes de)
[16] Re-activa: A favor que las políticas implementadas fueran re-activas (actuaran después de ejecutada la acción). (Después de).

Tabla 5. Descripción de los componentes para crear una política en el gestor

Elementos de una política	Definición
1. Identificativo (código política)	El identificátivo debe corresponder a una estructura de codificación que le permita al administrador del sistema realizar operaciones de consulta, búsquedas, modificaciones, etc, de una forma sencilla dentro de la base de datos que contiene la información correspondiente las políticas de seguridad.
2. Nombre (denominativo)	Por facilidad de administración, este nombre debe ser sencillo, conciso y concreto de tal manera que en la implementación del sistema de protección, pueda realizarse una referencia a un objeto de tipo política que contenga la información necesaria para ejecutar el control necesario de dicha directiva de seguridad. La sencillez de este denominativo también permitirá mayor eficiencia en la transacción de datos entre el gestor y el agente, además de facilitar las operaciones realizadas por el manejador de la base de datos.
3. Información adicional	Esta información permite tener un registro preciso de cada política que se desea implementar, como la fecha de creación, duración (si la política lo requiere), fecha de expiración (si la política lo requiere), estado de la política (activa/inactiva). La información detallada le permitirá al administrador llevar un control total de sus funciones de gestión, además de facilitar la elaboración de los reportes e informes estadísticos.

4. Alcance de la política	Este aspecto busca limitar la política a su objetivo en el sistema, sin tratar de abarcar otros aspectos que restarían eficiencia en tiempo de ejecución y que además pueden llegar a colapsar el sistema o incluso en estado de fuera de control la misma Red. Aunque esta información no forma parte de la implementación de las políticas, si se considera relevante para las correspondientes operaciones de gestión que realizará el Administrador en el momento de crear, modificar e implementar políticas de seguridad a través del módulo de gestión del sistema.
5. Objetivos de la política	Se considera el corazón estructural de la política y debe constituirse en una respuesta directa y suficiente frente a la falla o problema de seguridad que busca controlar. Su información es fundamental para la gestión de políticas aunque no se considere un requisito visible en la implementación del sistema más allá del correspondiente algoritmo de operación.
6. Descripción de los elementos involucrados en la política y su definición.	Esta información permite obtener una descripción detallada del contexto o entorno de operación del sistema gestor-agente además de los distintos actores que tendrán contacto con el sistema. También determina su comportamiento y funciones específicas frente a cada requerimiento de seguridad de la Red.
7. Definición de riesgos y consecuencias del no cumplimiento de la política	Esta información es relevante para realizar una correcta gestión de políticas que se ajuste a la realidad del sistema que se desea proteger en cuanto a desprotección e inseguridad, riesgos, fallos y vulnerabilidades que se desean erradicar o aminorar.
8. Aplicativos y/o sanciones	Este análisis debe proporcionar de forma precisa los medios operativos mediante los cuales se controlará el cumplimiento de las políticas de seguridad. Depende de una decisión del área

	administrativa de la Red o de la Organización quienes se responsabilizan por las sanciones asignadas a los distintos infractores, su magnitud y duración (en el caso de que las políticas implementadas tengan un carácter restrictivo), y además permitirán al usuario recibir ayuda y soporte en el uso de los servicios que presta la institución (en el caso de que las políticas tengan una naturaleza educativa).
9. Nivel de seguridad (alto/medio/bajo)	En toda política a gestionar o implementar, debe existir una valoración de riesgo o daño que corresponda a una estimación mas o menos precisa del grado de inseguridad o consecuencias perjudiciales que asume la institución en el caso de la infracción de una o algunas de las políticas de seguridad que se desean controlar.
10. Contenido	Esta información debe brindar una explicación comprensible y coherente (preciso sin entrar en tecnicismos y terminología judicial), que aclare los motivos y propósitos que constituyen la razón de ser de cada política.
11. Actualización conforme a los propósitos organizacionales	Toda política debe brindar la flexibilidad necesaria para que su funcionamiento se adecue a los distintos cambios tecnológicos que pueden implicar un crecimiento en los riesgos de protección que la organización desea controlar.
12. Autoridad aprobatoria o responsable	En toda política debe existir una entidad aprobatoria y responsable cuya autoridad dentro de la institución le acredita asumir la seguridad de la Red mediante distintos mecanismos de protección que aseguren el funcionamiento normal del sistema y el cumplimiento de los propósitos organizacionales.

3.7. Naturaleza de las Políticas de Seguridad

La naturaleza de las políticas de seguridad puede ser educativa, restrictiva o educativa y restrictiva de forma simultánea. Esto se convierte en un factor importante porque determina las fronteras y límites de interacción entre los usuarios y la Red. A nivel de implementación esto representaría ya una característica opcional que describe una serie de operaciones definidas por el Administrador de Red o el Administrador de Seguridad de la Red. En la siguiente tabla 6 se muestra lo descrito anteriormente.

Tabla 6. Naturaleza de las política a implementar en Hegcon-PS

politica	**educativo**	**restrictivo**
politicaUno	si/no	si/no
politicaDos	si/no	si/no
...	si/no	si/no
politiciaEnesima	si/no	si/no

Para realizar la clasificación de las políticas que el proyecto **HEGCON-PS**[17] implemento, se realizó un análisis de los siguientes criterios de selección que se presentan en la tabla7.

Tabla 7. Criterios de selección usados para la clasificación de las políticas en Hegcon-PS.

Criterios de Selección	Definición
Orden técnico	Donde se seleccionaron las directivas de seguridad que realmente se pueden controlar haciendo uso de componentes software y cuya información se encuentre localizada en memoria o esté en uso por parte del sistema operativo
Protección ante amenazas lógicas	Debido a la naturaleza software del proyecto, su alcance se limitará a operar netamente en el

[17] Hegcon –PS : Herramienta de gestión y Control de políticas de seguridad computacional.

	entorno de lógico de los servicios que presta la Red y mas específicamente sobre las plataformas operativas instaladas en los puntos donde se realizará el control de políticas.
Prioridad	Este elemento de análisis se definieron los propósitos del proyecto en torno a unos riesgos conocidos con anterioridad por parte de la red de datos de la universidad y que ya se consideran una necesidad cuya respuesta y solución mas eficiente y versátil se encuentran mediante la implementación de este proyecto.

Teniendo en cuenta los criterios de selección presentados en la tabla 6, se presentan en la tabla 8, las políticas piloto sobre las cuales se centro la implementación del proyecto **HEGCON-PS.**

Tabla 8. Políticas implementadas en Hegcon-PS

Políticas implementadas en Hegcon-PS
Política de operación de los Agentes (instalación, funcionamiento, mantenimiento)
Política sobre software autorizado
Política sobre accesos y usos de Servicios Internet
Política sobre Mecanismos de Protección (virus, troyanos, software malicioso, etc.)
Política de control sobre recursos compartidos

3.7.1. Estructuras las Políticas Implementadas en Hegcon-PS

Para las políticas implementadas se tienen objetivos y sanciones generales los cuales se describen en la tabla 9.

Tabla 9. Objetivos y sanciones generales de las políticas implementadas en Hegcon-PS

Alcance General	El alcance general busca que estas políticas controladas en toda la red, sobre los equipos que dispongan lícitamente de sistema operativo Windows 98 ya que es el sistema operativo licenciado por la Universidad del Cauca.
Sanciones Generales	Serán definidas una vez creadas las políticas de seguridad institucionales. Para este proyecto las sanciones son solo Educativas y no restrictivas.

1. Política de Operación de los Agentes de Control

Definimos en primera instancia la valoración de riesgos descrita en la tabla 10, y las estrategias de seguridad e implementación en la tabla 11 para la política de operación de agentes de control.

Tabla 10. Valoración de riesgos de la política de Agentes de Control

Valoración de riesgos de la política de Agentes de Control	
Riegos de la política de Agentes	El riesgo básico respecto al Agente de control es su desinstalación de forma voluntaria o involuntaria.
Prob. Ocurrencia	La ocurrencia de un evento de esta categoría es bajo ya que el agente encripta y oculta sus archivos de funcionamiento.
Tipo de Riesgo	roboInformación (valoración: alto) ataquesIntrusión (valoración: medio) fallasSistema (valoración: medio) equivocacionesUsuario (valoración: medio)

Tabla 11. Estrategias de seguridad e Implementación para la política de operación de los Agentes de control

Estrategias de seguridad e Implementación Para la Política de operación de los Agentes de control	
Identificativo	001
Nombre	politicaAgentes
Inf. adicional	**fechaCreacion**: aa/mm/dd **fechaExpiracion**: aa/mm/dd **estadoPol**: activa [si/no]
Objetivo	El propósito fundamental es oficializar la instalación de los Agentes en los equipos terminales de la Red para brindar un nivel de protección frente a la ausencia de buenos hábitos de uso de los servicios informáticos por parte de los usuarios.
Descripción	El Agente de Control iniciará su funcionamiento de forma paralela al Sistema Operativo del equipo terminal. No se permite la desinstalación o desactivación de funciones del Agente a menos de que esta operación sea aprobada por el administrador de la Red a través del Gestor del sistema.
Consecuencias	Falta de control de políticas de seguridad sobre el equipo que no ha instalado el agente o que ha modificado la operación normal del Agente.
Sanciones	**Educativas:** El Agente desplegará información visual para guiar al usuario respecto al uso correcto de los servicios de Red y del mismo software de protección.
Contenido	**Educativo** "**Sistema de Control de Políticas de Seguridad Informática de la Red de Datos de la Universidad del Cauca.** **Política de Seguridad No**. 001 **Elaborada por**: Red de Datos Unicauca **Aprobada por**: Comité Verificador

	Fecha de Operación fechaCreacion **Política de Agentes de Control** Esta política establece de forma institucional la operación de los Agentes de control en cada uno de los equipos de la Red que tienen instalado el sistema operativo Windows 98 y le permitirá a cada usuario hacer un uso correcto de los servicios prestados por la Red de Datos de la Universidad del Cauca. No trate de desinstalar el Agente, ni modificar su correcto funcionamiento.
Actualización	A disposición del Administrador de Red a través del Módulo de gestión (según una opción seleccionada por el Administrador en el momento de gestionar y crear la política de seguridad)
Aprobador	Comité Verificador Administración Red de Datos Unicauca

2. Política de Monitoreo sobre el Software Instalado en los Equipos Terminales de la Red, el Software Licenciado, y el Software que Debilita la Protección de la Red.

Definimos en primera instancia la valoración de riesgos descrita en la tabla 12, y las estrategias de seguridad e implementación en la tabla 13 para la política de monitoreo de software.

Tabla 12. Valoración de riesgos de la política de monitoreo de software.

Valoración de riesgos de la política de Monitoreo de software	
Riegos de la política de Monitoreo se software.	El riesgo básico respecto al software instalado en los equipos terminales se remite al software instalado sin autorización por parte de la Administración de la Red de Datos. La institución está en la obligación de controlar qué software está autorizado para ser instalado y que programas se consideran no válidos o peligrosos para el sistema por incurrir en algún tipo de

	amenaza para la seguridad de la Red.
Prob. Ocurrencia	La actividad de instalación de software sin autorización e instalación de software no licenciado, además de software no confiable o inseguro es talvez una de las más habituales, y la implantación de una contramedida o control es cada vez mas urgente.
Tipo de Riesgo	FraudeLegal(valoración: medio) FallasSistema(valoración: medio) ProgramasMaliciosos(valoración: medio) AccesoNoAutorizado(valoración: medio)

Tabla 13. Estrategias de seguridad e Implementación para la política de monitoreo

Estrategias de seguridad e Implementación Para la política de Monitoreo de software	
Identificativo	002
Nombre	Política de control software instalado
Inf. adicional	**fechaCreacion**: aa/mm/dd **fechaExpiracion**: aa/mm/dd **estadoPol**: activa [si/no]
Objetivo	El propósito fundamental es que la Administración de la Red pueda tener un control sobre el tipo de software que se instala en los equipos terminales, permitiendo o denegando la instalación de ciertos programas que pueden atentar contra la seguridad de la Red de Datos.
Descripción	El Agentes está encargado de llevar a cabo una evaluación exhaustiva y control del software instalado en el equipo, software licenciado, software permitido y no permitido. El Gestor posee en su base de datos una lista estándar del software licenciado y aprobado por el comité aprobador (Directivas de la Institución), y esta lista es suministrada a cada uno de los

	Agentes. El Agente de Control instado en el equipo terminal revisa en el registro del Sistema Operativo que software se encuentra actualmente instalado, y notifica al Usuario Responsable (monitor, laboratorista, encargado) el software que se encuentre como no autorizado en el momento de la instalación del Agente.
Consecuencias	El incumplimiento de esta política pone en riesgo tanto la credibilidad institucional, como los gastos que se derivan por penalizaciones a las normas constitucionales que protegen los derechos de autor, además de que la ejecución de programas no confiables amenaza la protección del sistema.
Sanciones	**Educativo.**El Agente desplegará información visual para guiar al usuario respecto al uso correcto de los servicios de Red y del mismo software de protección. Además el Agente notificará al usuario algunas operaciones que no se deben realizar, como por ejemplo tratar de desinstalar el software sin autorización, o instalar software que la Red de Datos ha catalogado como no confiable o perjudicial para la Red.
Contenido	**Educativo** "**Sistema de Control de Políticas de Seguridad Informática de la Red de Datos de la Universidad del Cauca Política de Seguridad No**. 002 **Elaborada por**: Red de Datos Unicauca **Aprobada por**: Comité Verificador **Fecha de Operación :** fechaCreacion Esta política establece de forma institucional que tipo de software esta autorizado por parte de la Administración de la Red de Datos para ser instalado en los equipos terminales de la Red.
Actualización	A disposición del Administrador de Red a través del Módulo de gestión (según una opción seleccionada por el Administrador en el momento de gestionar y crear la política de seguridad)
Aprobador	Comité Verificador Administración Red de Datos Unicauca

3. Sobre Restricción y Control de Visitas a Sitios Web no Autorizados.

Definimos en primera instancia la valoración de riesgos descrita en la tabla 14, y las estrategias de seguridad e implementación en la tabla 15 para la política de control de acceso a sitios web no autorizados.

Tabla 14. Valoración de riesgos de la política control de visitas a sitios Web no autorizados

Valoración de riesgos de la política visitas a sitios Web no autorizados	
Riegos de la política visitas a sitios Web no autorizados.	Se hace necesario concienciar sobre los criterios que tiene la organización para realizar las actividades de "navegación" en la red, no se puede discriminar de forma directa las intenciones de un usuario al navegar por la red, pero se intenta educar a los usuarios sobre la mejor forma de utilizar estos servicios..
Prob. Ocurrencia	Dependiendo de la facilidad de acceso por parte de los usuarios a conexiones externas a la Intranet (lo que sucede en la mayoría de los sistemas LAN ya que el acceso a internet es atractivo para cualquier organización), por lo general la probabilidad de ocurrencia es alta.
Tipo de Riesgo	FraudeLegal(valoración: medio) FallasSistema(valoración: medio) ProgramasMaliciosos(valoración: medio) AccesoNoAutorizado(valoración: medio)

Tabla 15. Estrategias de seguridad e Implementación para la política control de visitas a sitios

Estrategias de seguridad e Implementación Para la política de control de visitas a sitios web no autorizados	
Identificativo	003
Nombre	Política sobre uso de Servicios Internet
Inf. adicional	**fechaCreacion**: aa/mm/dd **fechaExpiracion**: aa/mm/dd **estadoPol**: activa [si/no]
Objetivo	El propósito fundamental es que la Administración de la Red pueda tener un control sobre el uso de los servicios internet en cada uno de los equipos terminales, verificando además que para su correcto funcionamiento el software de navegación esté correctamente configurado y actualizado
Descripción	El Agente chequeará los registros de información sobre las actividades por parte del usuario al incursionar en los servicios Internet, comparará con los patrones asignados por el gestor, emitiendo la correspondiente información acerca de las infracciones y usos indebidos por parte del usuario (acceso a través de servicios Internet a sitios reconocidos con contenido perjudicial para el usuario, la Red o la misma Organización).
Consecuencias	El incumplimiento de esta política pone en riesgo tanto la información organizacional, como el correcto funcionamiento del sistema e incluso de la red.
Sanciones	**Educativo** El Agente desplegará información visual para guiar al usuario respecto al uso correcto de los servicios Internet educándole así mismo acerca de los riesgos y perjuicios por un mal uso de los servicios Internet. Además el Agente notificará al usuario algunas operaciones que no se deben realizar, como por ejemplo descarga de información si un previo chequeo antivirus. .
Contenido	**Educativo** "**Sistema de Control de Políticas de Seguridad Informática de la Red de Datos de la Universidad del Cauca**

	Política de Seguridad No. 003 **Elaborada por**: Red de Datos Unicauca **Aprobada por**: Comité Verificador **Fecha de Operación :** fechaCreacion Esta política establece de forma institucional que debe limitarse el uso de los servicios Internet para usos académicos, investigativos o aquellos que correspondan con el carácter institucional.
Actualización	A disposición del Administrador de Red a través del Módulo de gestión (según una opción seleccionada por el Administrador en el momento de gestionar y crear la política de seguridad)
Aprobador	Comité Verificador Administración Red de Datos Unicauca

4. Sobre los Mecanismos de Protección contra Virus Informáticos.

Definimos en primera instancia la valoración de riesgos descrita en la tabla 16, y las estrategias de seguridad e implementación en la tabla 17 para la política de que implementa mecanismos de protección contra virus informáticos.

Tabla 16. Valoración de riesgos de la política que implementa mecanismos de Protección contra virus Informáticos.

Valoración de riesgos de la política que implementa mecanismos de Protección contra Virus Informáticos.	
Riegos de la política que implementa mecanismos de Protección contra virus Informáticos	Tal vez uno de los riesgos mas amplios en el uso no controlado de los recursos de red por parte de los usuarios está en el alto grado de desconocimiento respecto a las amenazas directas contra los sistemas como son los programas y códigos maliciosos, entre ellos

	podríamos destacar los virus, troyanos y gusanos informáticos, esta política verifica que en todos los equipos estén instalados antivirus con sus respectivas actualizaciones.
Prob. Ocurrencia	Dependiendo de la facilidad de acceso por parte de los usuarios a conexiones externas a la intranet (lo que sucede en la mayoría de los sistemas LAN ya que el acceso a Internet es atractivo para cualquier organización), por lo general la probabilidad de ocurrencia es alta (eso sin contar los casos sin documentar).
Tipo de Riesgo	FraudeLegal(valoración: medio) FallasSistema(valoración: medio) ProgramasMaliciosos(valoración: medio)

Tabla 17. Estrategias de seguridad para la política de Protección contra Virus Informáticos

Estrategias de seguridad e Implementación Para la política Mecanismos de Protección contra Virus Informáticos	
Identificativo	004
Nombre	Mecanismos de Protección contra Virus Informáticos.
Inf. adicional	**fechaCreacion**: aa/mm/dd **fechaExpiracion**: aa/mm/dd **estadoPol**: activa [si/no]
Objetivo	El propósito fundamental es que la Administración de la Red pueda tener un control sobre los mecanismos de protección instalados en los equipos terminales, verificando además que para su correcto funcionamiento estos paquetes software estén correctamente configurados y actualizados.
Descripción	El Agente chequeará dentro del software del equipo Terminal la existencia o no de los paquetes software de protección suministrados por parte del Administrador como una lista válida de software que debería estar instalado en el sistema. Además, accediendo a registro del sistema operativo, también podrá verificar que estos paquetes software estén correctamente

	instalados y configurados. Se notifica al usuario responsable (monitor, laboratorista, encargado) el software que no se encuentre o que requiera configuración y/o actualización.
Consecuencias	El incumplimiento de esta política pone en riesgo tanto la información organizacional, como el correcto funcionamiento del sistema e incluso de la red.
Sanciones	**Educativo** El Agente desplegará información visual para guiar al usuario respecto al uso correcto de los servicios de Red y del mismo software de protección. Además el Agente notificará al usuario algunas operaciones que no se deben realizar, como por ejemplo tratar de desinstalar el software sin autorización, o instalar software que pone el riesgo el rendimiento del sistema (como se da en el caso de la instalación simultanea de dos o mas antivirus, o de dos o mas firewalls).
Contenido	**Educativo** "**Sistema de Control de Políticas de Seguridad Informática de la Red de Datos de la Universidad del Cauca** **Política de Seguridad No**. 004 **Elaborada por**: Red de Datos Unicauca **Aprobada por**: Comité Verificador (¿?) **Fecha de Operación:** fechaCreacion Esta política establece de forma institucional que tipo de software cuya instalación y funcionamiento es requerido por parte de la Administración de la Red de Datos sobre los equipos terminales de la Red.
Actualización	A disposición del Administrador de Red a través del Módulo de gestión (según una opción seleccionada por el Administrador en el momento de gestionar y crear la política de seguridad)
Aprobador	Comité Verificador Administración Red de Datos Unicauca

5. Política Sobre el Control de los Recursos Compartidos (carpetas e impresoras).

Definimos en primera instancia la valoración de riesgos descrita en la tabla 18, y las estrategias de seguridad e implementación en la tabla 19 para la política de control de recursos compartidos.

Tabla 18. Valoración de riesgos de la política que implementa mecanismo de control sobre los recursos compartidos.

Valoración de riesgos de la política que implementa mecanismos de control de recursos compartidos	
Riegos de la política que implementa mecanismos de control de recursos compartidos.	Una de la fallas de seguridad reconocida en los sistemas Windows es la vulnerabilidad en los protocolos de acceso a recursos compartidos, lo cual permite que si un intruso consigue afectar un equipo fácilmente consiga tener dominio y control sobre equipos que no están correctamente configurados, incluso varios gusanos han logrado aprovechar este bug para realizar actividades hostiles y de control.
Prob. Ocurrencia	No es habitual en redes LAN de pequeña envergadura, sin embargo en grandes Redes LAN's o en Redes Interconectadas, la probabilidad de encontrar y vulnerar este fallo de seguridad alcanza niveles medianamente altos.
Tipo de Riesgo	FraudeLegal(valoración: alta) FallasSistema(valoración: medio) ProgramasMaliciosos(valoración: medio) accesoNoAutorizado (valoración: medio)

Tabla 19. Estrategias de seguridad e Implementación para la política control de

Estrategias de seguridad e Implementación Para la política de control de los recursos compartidos	
Identificativo	005
Nombre	Política sobre Recursos Compartidos
Inf. adicional	**fechaCreacion**: aa/mm/dd **fechaExpiracion**: aa/mm/dd **estadoPol**: activa [si/no]
Objetivo	El propósito fundamental es que la Administración de la Red pueda tener un control sobre los recursos compartidos en cada uno de los equipos terminales, verificando además la correcta configuración de estos en el caso de ser necesario.
Descripción	El Agente chequeará los registros de información sobre los servicios de red buscando recursos compartidos de forma innecesaria, o configuraciones incorrectas del sistema de recursos compartidos para controlar que este fallo de seguridad no sea vulnerado de alguna forma..
Consecuencias	El incumplimiento de esta política pone en riesgo tanto la información organizacional, como el correcto funcionamiento del sistema e incluso de la red.
Sanciones	Educativo: El Agente desplegará información visual para guiar al usuario respecto al uso correcto de los servicios de Red y en este caso específico si se hace necesario sobre los riesgos en la compartición de recursos y una configuración incorrecta del sistema.
Contenido	**Educativo** "**Sistema de Control de Políticas de Seguridad Informática de la Red de Datos de la Universidad del Cauca** **Política de Seguridad No**. 005 **Elaborada por**:Red de Datos Unicauca **Aprobada por**: Comité Verificador **Fecha de Operación :**fechaCreacion Esta política establece de forma institucional que debe limitarse

	el uso de los servicios de Red como los recursos compartidos con el fin de centrar su uso en actividades de naturaleza académica, investigativa o aquellas que correspondan con el carácter institucional.
Actualización	A disposición del Administrador de Red a través del Módulo de gestión (según una opción seleccionada por el Administrador en el momento de gestionar y crear la política de seguridad)
Aprobador	Comité Verificador Administración Red de Datos Unicauca

4. PSEUDO-LENGUAJE DE OPERACIÓN

El primer paso para dotar de flexibilidad a Hegcon-PS es la implementación de un sistema de comunicación que pueda darle poder al agente para interpretar y además eso, libertad al gestor para expresar los fundamentos conceptuales de las políticas informáticas a través de medios lógicos.

No se tomó un sistema de protocolos pues estos son rígidos y se basan en longitudes y parámetros limitados. La investigación utilizó las metodologías formales de BNF (*Backus Naun Form*) y análisis sobre gramáticas formales. [7]

Este sistema de comunicación establece un modelo de interacción entre el Gestor y el Agente. Para definir este protocolo es necesario realizar un análisis de los mensajes intercambiados entre el Gestor y el Agente, además de la constitución semántica de cada uno de estos mensajes. Cada mensaje esta compuesto por segmentos de trama de tipo String (cadena de caracteres) que poseen una semántica definida y que asociadas determinan el comportamiento del sistema frente a ciertos parámetros o argumentos.

Un segmento completo puede contener la información de operaciones a realizar de forma dinámica, o de operaciones de control que se escribirán de forma estática en la estructura de archivos que componen la SIB[18] del Agente. Para lograr que el pseudo-lenguaje de operación sea flexible, se debe implementar un intérprete o módulo de interpretación de protocolo en cada agente, capaz de analizar la sintaxis correspondiente a la trama de información transferida desde el Gestor y de realizar las operaciones correspondientes.

[18] SIB: Base de datos donde se guarda información de las políticas de seguridad y resultados de la aplicación de las mismas

Es necesario distinguir entre el protocolo de comunicación que utilizan el Gestor y el Agente para realizar la correspondiente transferencia de información (protocolo de comunicación facilitado por RMI llamado Rmi.protocol, soportado sobre la plataforma Tcp/Ip) y el pseudo-lenguaje de operación que se implementará para desfragmentar e interpretar la información recibida de forma dinámica o que se ha escrito en la estructura de archivos del SIB del Agente.

En general, las tramas contienen información relativa a las políticas. Para lograr una estandarización de las distintas funcionalidades del sistema que se gestionarán de forma dinámica a través de este pseudo-lenguaje, se realizará un análisis sintáctico y semántico de los requerimientos de una política de seguridad en general, independientemente del tipo de control o propósito de cada política de forma específica.

Este análisis tratará de abarcar todos los aspectos de administración de seguridad entorno a las políticas de seguridad piloto propuestas por el proyecto HEGCON-PS, lo que no significa que no se puedan realizar desarrollos para explotar el pseudo-lenguaje y maximizar las funciones del sistema, con la implementación de nuevas políticas de seguridad.

Primero que todo se requiere unas definiciones que se presentan a continuación:

Operación: Se define como una unidad sintáctica con un significado concreto y que puede estar provista o no de ciertos parámetros y/o argumentos. Un segmento de trama completo debe estar definido entre separadores de tipo “»” que significa que todo su contenido tanto de aplicación como información correlativa esta totalmente incluida dentro de dichos separadores. Generalmente cada segmento de trama lleva un descriptor que define la naturaleza de cada política de tal manera que facilita al Administrador las labores de gestión de políticas para que no se realicen encadenamientos de

segmentos de forma aleatoria, lo cual puede repercutir en una trama que carece de significado o inoperable.

Objeto: Se define como un elemento determinado y que complementa o define la información de una determinada operación. El valor debe corresponder a una serie de opciones de objetos que se aceptan como válidas para ser interpretadas dentro de la trama y corresponde a una instancia puntual de un cierto aspecto o elemento que se desea cuantificar.

4.1. Definición Lenguaje de Políticas de Seguridad (lps)

4.2. Introducción.

En esta parte trabajaremos la estructura que conforma el lenguaje de políticas de seguridad computacional que se implemento en el gestor para que fuese interpretado por el agente, con este lenguaje se crean las políticas de seguridad que definen los administradores de la red para controlar y educar a los usuarios de la red de la universidad del cauca.

4.2.1. Header o Cabecera de política

Contiene la información estandarizada que maneja toda política implementada, que consiste en el estado de la política (STD), el título de la política (TTL), el código de la política (COD), el autor o diseñador de la política (AUT), el ente aprobador de la política (APR), la naturaleza de la política (CLS), la fecha de inicio de operación de la política (DTI), la fecha de expiración o término de vigencia de la política (DTE), el nivel de riesgo o nivel de seguridad de la política (RSK), el tiempo o intervalo de control de la política (TMC), la información de contenido que explica la política (INF). Todos estos términos, operadores y operandos contienen información estática y se explicarán de forma detallada en las secciones posteriores. La información incluida en la cabecera, se incluye en la SIB

solo una vez, y no se hace control sobre ella pues se considera estática. La trama correspondiente se muestra a continuación:

"**HDR**" **HEADER**. Esta cadena contiene los valores:

STD + TTL + COD + AUT + APR + CLS + DTI + DTE + RSK + TMC + INF + OPR

Donde OPR(operación) puede ser opcional según los requerimientos de la implementación de la política.

4.2.2. Título de la Política

El Diseñador de políticas tiene la opción de etiquetar cada política bajo un título que se considerará de forma oficial como el nombre con el cual se reconocerá la política, aunque no se utilizará para efectos de indexación, para lo cual resulta mucho más efectivo trabajar con el código (COD) de la política. El valor de esta trama debe ir especificado dentro del operando "TTL", cuyo argumento asume como valor el String que asigne el diseñador. El intérprete de tramas sabe que esta información forma parte de la cabecera y asocia dicho título al procedimiento que constituye la política. A continuación se presenta la descripción de la trama:

TTL / Titulo

La sintaxis es la siguiente:

TTL=String que especifica el título de la política

En este ejemplo se asignará el título a una política que se utilizará para controlar el software instalado en los equipos de la Red

TTL=Política de Control de Software Instalado en los Equipos de la Red

---

4.2.3. Código de la política

Este código debe ser obligatoriamente implementado ya que se utilizará para realizar indexaciones en procesamiento de datos.

COD / Código. Especifica el Código asignado por el Administrador o diseñador de la política. Esta codificación se puede realizar asignando registros de tipo numérico o cadenas de caracteres con contenido administrativo. En el caso del sistema **Hegcon-PS** la asignación de código se realizará concatenando la información correspondiente al edificio, piso y número de oficina donde se encuentra el equipo además de el código de punto de red y la dirección física o MAC del equipo donde se instala el Agente de Control. La sintaxis es la siguiente:

COD=*Valor de código (String) asignado para esta política*

Este es un ejemplo de asignación de código para la política que se está trabajando dentro del ejemplo:

COD=INGENIERÍAS-3-329-06-FF-DD-EE-C0-0A-B6

4.2.4. Autor de la Política

Especifica quién fue el directo encargado del diseño e implementación de la política haciendo uso de la herramienta HEGCON-PS.

A continuación se describe la trama.

"**AUT**" **AUTOR**. Esta trama especifica en el String que toma como valor el autor oficial de la política, quien la diseñó y la implementó en el sistema HEGCON-PS. La sintaxis es la siguiente:

AUT=”Nombre del Autor de la política”

En este ejemplo se le asigna el autor a la política que se implementará

AUT= “Red de Datos Unicauca”

4.2.5. Aprobador de la Política

Especifica quién fue el directo encargado de aprobar oficialmente la implementación de la política y debe ser un ente oficialmente reconocido dentro de la entidad.

A continuación se describe la trama.

“**APR**” **APROBADOR**. Esta trama especifica en el String que toma como valor el aprobador oficial de la política. La sintaxis es la siguiente:

APR=”Nombre del Aprobador oficial de la política”

En este ejemplo se le asigna el autor a la política que se implementará

APR= “Vicerectoría de Investigaciones”

4.2.6. Naturaleza de la política

El Autor o diseñador de políticas en conjunto con el Aprobador debe elegir la naturaleza de las políticas que se implementarán según especifica la trama que se describe a continuación.

CLS / Clase. Define el carácter de la política, que puede tener dos órdenes de control, de tipo educativo o educativo-restrictivo. El tipo educativo debe añadir la información que se

desea desplegar de forma visual para guiar al usuario en el cumplimiento de las políticas o informar de su infracción.

El tipo restrictivo debe añadir la información que contiene la secuencias de control que ejecutan operaciones sobre el sistema operativo (por ejemplo denegando la autorización para la visita de un sitio web específico, o impidiendo la ejecución de un programa software determinado, o entrar en estado de espera hasta que el usuario realice una operación solicitada, en realidad depende del grado de restricción que el Administrador desee implementar para la protección de la Red).

Existe un tipo híbrido que asume los dos modelos; educativo + restrictivo y que toma los dos tipos de control de la política. Este segmento de trama es obligatorio, no secuencial y puede tomar tres valores: “EDU” si se desea implementar la política de forma Educativa, “RES” si se desea implementar la política solo de forma Restrictiva y “HYB” si se desea implementar la política de forma educativa y restrictiva simultáneamente.

Descripción de los posibles valores

EDU / Educativo. El carácter de la política que se está implementando es solo de tipo educativo, lo que significa que no existirán operaciones de restricción sobre ciertas funciones del sistema operativo. Se manejará información de tipo visual que se desplegará en el momento de una solicitud por parte de un usuario para recibir información acerca de las políticas, o en el caso de una infracción de dicha política.

RES / Restrictiva. El carácter de la política es de tipo restrictivo, y si se elige esta opción, se debe suministrar las distintas operaciones de control que constituirán la sanción a la infracción cometida. Este criterio de restricción está sujeto al criterio del diseñador de políticas en conjunto con el Aprobador. No se requiere despliegue de información como en el parámetro educativo, pues en un momento determinado el Administrador de la Red puede considerar urgente realizar el control de ciertas operaciones de seguridad sin que sea requisito dar información de estas operaciones a los usuarios.

HYB / Híbrida. Cuando el carácter de la política es educativo y restrictivo de forma simultánea. Debe suministrar tanto la información a desplegar como las operaciones que constituirán la sanción a la infracción cometida.

La sintaxis es la siguiente según la decisión del diseñador o autor de la política:
CLS="**EDU**" //política de orden educativo
CLS="**RES**" //política de orden restrictivo
CLS="**HYB**" //política de orden educativo y restrictivo

4.2.7. Fecha de /Expiración

o término de la vigencia de la Política. (DTE-DTI)

Se utiliza estas tramas para especificar la fecha exacta de inicio de operación de la política implementada y también la fecha exacta de caducidad de la política. El formato de la fecha debe corresponder al estándar que utiliza el gestor de base de datos utilizado en el módulo de gestión del proyecto (en este caso MySql). La trama se describe a continuación

"**DTI**" **FECHA INICIO**. Cuya sintaxis es: DTI="*aaaa-mm-dd*"
"**DTE**" **FECHA EXPIRACIÓN**. Cuya sintaxis es: DTE="*aaaa-mm-dd*"
Para el ejemplo que se está desarrollando, la sintaxis correspondiente sería

DTI="2003-06-01"
DTE="2004-06-01"

NOTA: Como recomendación de los diseñadores del proyecto HEGCON-PS, el tiempo prudencial para la implementación de una política debe corresponder al intervalo aproximado de un año, tras lo cual se recomienda evaluar la efectividad, utilidad y comportamientos anormales como resultado de la implementación de la política.

4.2.8. Riesgo de la política

Define una valoración del riesgo o peligrosidad de la infracción de una política. A continuación se describe su correspondiente segmento de trama.

"**RSK**" **RIESGO**. Asume tres valores. Estos valores están sujetos al criterio del diseñador de la política. Los tres posibles valores son:

"**HGH**" **HIGH**. Alto riesgo de peligrosidad
"**MID**" **MIDDLE**. Riesgo de peligrosidad: medio
"**LOW**" **LOW**. Bajo riesgo de peligrosidad

La sintaxis, dependiendo del valor asumido por el diseñador sería:

RSK="**HGH**" //*Riesgo Alto*
RSK="**MID**" //*Riesgo Medio*
RSK="**LOW**" //*Riesgo Bajo*

4.2.9. Tiempo de Control de la política

En razón del rendimiento del equipo sobre el cual se está controlando la política, no se considera necesario estar realizando una lectura permanente del sistema (registro del sistema operativo o del sistema de archivos), ya que esto podría sobrecargar el sistema y perjudicar su rendimiento, por lo cual se brinda la opción de realizar chequeos periódicos según el diseñador de políticas considere necesario. Este periodo debe estar especificado en milisegundos. A continuación se describe la trama.

"**TMC**" **TIEMPO CONTROL**. Especifica en su argumento el intervalo para realizar el chequeo de cumplimiento del procedimiento que constituye la política. Solo las

operaciones descritas dentro del procedimiento (PRS) serán ejecutadas en de forma continua y persistente en este intervalo de tiempo. Por ello se debe ser cuidadoso en especificar bien las operaciones (OPR) que se consideran necesarias para controlar de forma continua la política (pues se permite realizar operaciones fuera del procedimiento de control de la política, como escribir archivos, cuya información no requiere modificarse y por lo tanto no se necesita realizar dicha operación sino solo una vez. La sintaxis es la siguiente:

TMC="*Tiempo especificado en milisegundos y debe ser un entero*"

La aplicación al ejemplo que se ha venido trabajando tomará como intervalo de control un periodo de 10 minutos que corresponde a 600000 milisegundos.

TMC="600000"

4.2.10. **Información de la política**

Toda política que se implemente debe suministrar la información que corresponda a su contenido explicativo, lo cual facilita mantener tanto para el diseñador como para los usuarios la opción de comprender el planteamiento conceptual de la política que se está implementando. La trama está descrita de la siguiente forma:

"**INF**" **INFORMACIÓN**. Esta información debe consignarse según el estándar java para la presentación de Strings con sus correspondientes secuencias de escape. La sintaxis es la siguiente:

INF="Aquí se consigna la información explícita\n
que contiene el planteamiento conceptual\n
sobre el cual se diseñó esta política."

4.2.11. Operaciones

Son actividades específicas que se realizan de forma puntual. Y están constituidas por sentencias específicas concatenadas por el signo (+) y que mientras estas sentencias estén dentro de la misma operación el resultado obtenido se almacenará en un objeto temporal llamado RSL. Debido a esto la recomendación es que las sentencias que constituyen cada operación trabajen en torno al mismo objeto, pues el objeto RSL solo tiene cobertura local, y si se define una operación que arrojará un nuevo tipo de resultado existirán incompatibilidades. Si se quiere trabajar sobre un nuevo objeto y se usará la variable RSL, se necesita declarar una nueva operación, ya que para cada operación el valor de RSL se vacía. Las distintas operaciones se describirán en detalle a continuación, especificando el tipo de objeto sobre el cual trabajan, y los distintos parámetros y argumentos que requieren.

A continuación se presenta la lista de operaciones admitidas por el pseudo-lenguaje de operación implementado en el proyecto HEGCON-PS.

“EJECUTAR”	**EJECUTAR**
“LEER”	**LEER**
“ESCRIBIR”	**ESCRIBIR**
“BUSCAR”	**BUSCAR**
“ADICIONAR”	**ADICIONAR**
“COMPARAR”	**COMPARAR**
“EQUALIZAR”	**EQUALIZAR**
“DESPLEGAR”	**DESPLEGAR**
“COMANDO”	**COMANDO**
“ELIMINAR”	**ELIMINAR**

Estas operaciones se especifican de forma detallada en los siguientes apartados.

OPERANDOS

Se utilizan los operandos como argumentos en los parámetros que reciben las operaciones especificadas por los operadores anteriormente descritos. Los operadores se listan a continuación.

"**ARCHIVO**"	Especifica un objeto de tipo archivo
"**DIRECTORIO**"	Especifica un objeto de tipo directorio del sistema
"**CLAVE**"	Especifica todos los objetos contenidos en una clave del registro
"**VALOR**"	Especifica el contenido de un valor del registro especificado en su nombre
"**MENSAJE**"	Especifica un mensaje de tipo String. Se puede especificar dentro de los objetos tipo MENSAJE que la cadena sea específicamente el usuario activo en el sistema operativo, o la fecha actual del sistema, e incluso el código del Agente.

"**FECHA**" Especifica un objeto tipo date que toma como parámetros:

AA	Año ej:[2003]
AA/MM	Año/Mes ej:[2003/11]
AA/MM/DD	Año/Mes/Día ej:[2003/11/20]
AA/MM/DD/HH	Año/Mes/Día/Hora ej:[2003/11/20/9]
AA/MM/DD/HH/MN	Año/Mes/Día/Hora/Minutos ej:[2003/11/20/9/35]
AA/MM/DD/HH/MN/SS	Año/Mes/Día/Hora/Minutos/Seg ej:[2003/11/20/9/35/4]

USUARIO.	Especifica un objeto que contiene el usuario actual y sirve para notificar sobre una actividad y el usuario que la realizó (por ejemplo las infracciones).

4.3 Reglas de Producción Para Lenguaje de Políticas de Seguridad (LPS)

1. <PROCEDIMIENTO> -> {<OPERACION>;<N>}

2. <OPERACION> -> <tipoOperacion>[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

3. <OPERACION> -> <tipoOperacion>[<tipoObjeto>(“<objeto>”)]

4. <OPERACION> -> <tipoOperacion>[RESULTADO, <tipoObjeto>(“<objeto>”)]

5. <N> -> <OPERACION>

6. <N> -> ;

7. <N> -> ø

8. <tipoObjeto> -> ARCHIVO | DIRECTORIO | MENSAJE | CLAVE | VALOR

9. <tipoOperacion> -> EJECUTAR | IMPORTAR | LEER | ESCRIBIR | ADICIONAR
| COMPARAR | EQUALIZAR | ELIMINAR | COMANDO
| REPORTAR | DESPLEGAR

10. <objeto> -> literalCadena

Donde:

letra -> [a-zA-Z]

digito -> [0-9]

literalCadena -> letra < letra | digito >

NOTA: Los objetos deben corresponder a Objetos del Sistema de Archivos o del Registro de Configuraciones.

4.4 Gramática Lps Para las Operaciones en Lps

4.4.1. Ejecutar

Aplicar 3.

<OPERACION> -> EJECUTAR[<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> EJECUTAR[VALOR(“<objeto>”)]

Aplicar 10.

<OPERACION> -> EJECUTAR[VALOR(“SI”)]

NOTA: Cuando se realiza una Operación EJECUTAR, el valor solo puede tomar dos valores “SI”, o “NO”.

4.4.2. Importar

Aplicar 2.

<OPERACION> -> IMPORTAR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> IMPORTAR[ARCHIVO(“<objeto>”),ARCHIVO(“<objeto>”)]

Aplicar 10.

NOTA: El objeto ARCHIVO puede especificar la ruta de dónde se importa el archivo y en donde se lo va a ubicar.

4.4.3. Leer

Aplicar 2.

<OPERACION> -> LEER[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> LEER[ARCHIVO(“<objeto>”),DIRECTORIO(“<objeto>”)]

lee un archivo de un directorio y lo almacena en la variable temporal RESULTADO

Aplicar 8.

<OPERACION> -> LEER[DIRECTORIO(“<objeto>”),DIRECTORIO(“<objeto>”)]

lee un directorio dentro de una ruta y almacena un lista de archivos en la variable RESULTADO

Aplicar 8.

<OPERACION> -> LEER[VALOR(“<objeto>”),CLAVE(“<objeto>”)]

lee un valor dentro de una clave y almacena su contenido en la variable RESULTADO

Aplicar 8.

<OPERACION> -> LEER[CLAVE(“<objeto>”),CLAVE(“<objeto>”)]

lee una clave dentro de una ruta y almacena la lista de valores y subclaves en la variable RESULTADO

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.4. Escribir

Aplicar 2.

<OPERACION> -> ESCRIBIR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> ESCRIBIR[ARCHIVO(“<objeto>”),DIRECTORIO(“<objeto>”)]

Escribe un archivo sin datos en un directorio

Aplicar 8.

<OPERACION> -> ESCRIBIR[VALOR(“<objeto>”),CLAVE(“<objeto>”)]

Escribe un valor sin contenido dentro de una clave del registro de configuraciones

Aplicar 4.

<OPERACION> -> ESCRIBIR[RESULTADO, <tipoObjeto>(“<objeto>”)]

Escribe el contenido actual de la variable RESULTADO en el <tipoObjeto> especificado

Aplicar 8.

<OPERACION> -> ESCRIBIR[RESULTADO, ARCHIVO(“<objeto>”)]

Escribe el contenido actual de la variable RESULTADO en el ARCHIVO especificado

Aplicar 8.

<OPERACION> -> ESCRIBIR[RESULTADO, VALOR(“<objeto>”)]

Escribe el contenido actual de la variable RESULTADO en el VALOR dentro del registro de configuraciones especificado

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.5. Adicionar

Aplicar 2.

<OPERACION> -> ADICIONAR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> ADICIONAR[ARCHIVO(“<objeto>”),DIRECTORIO(“<objeto>”)]

Adiciona un archivo sin datos en un directorio

Aplicar 8.

<OPERACION> -> ADICIONAR[VALOR(“<objeto>”),CLAVE(“<objeto>”)]

Adiciona un valor sin contenido dentro de una clave del registro de configuraciones

Aplicar 8.

<OPERACION> -> ADICIONAR[MENSAJE(“<objeto>”),VALOR(“<objeto>”)]

Adiciona una cadena como contenido al valor dentro de una clave del registro de configuraciones

Aplicar 8.

<OPERACION> -> ADICIONAR[MENSAJE(“<objeto>”),ARCHIVO(“<objeto>”)]

Adiciona una cadena dentro de un ARCHIVO en el sistema de archivos

Aplicar 4.

<OPERACION> -> ADICIONAR[RESULTADO, <tipoObjeto>(“<objeto>”)]

Adiciona el contenido actual de la variable RESULTADO en el <tipoObjeto> especificado

Aplicar 8.

<OPERACION> -> ADICIONAR[RESULTADO, ARCHIVO(“<objeto>”)]

Adiciona el contenido actual de la variable RESULTADO en el ARCHIVO especificado

Aplicar 8.

<OPERACION> -> ESCRIBIR[RESULTADO, VALOR(“<objeto>”)]

Adiciona el contenido actual de la variable RESULTADO en el VALOR dentro del registro de configuraciones especificado

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.6. Comparar

Aplicar 2.

<OPERACION> -> COMPARAR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> COMPARAR[ARCHIVO(“<objeto>”),ARCHIVO(“<objeto>”)]

Compara el ARCHIVO especificado en el primer argumento con el ARCHIVO especificado en el segundo argumento y busca los elementos del primer archivo que no existen en el segundo archivo

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.7. Equalizar

Aplicar 2.

<OPERACION> -> EQUALIZAR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> EQUALIZAR[ARCHIVO(“<objeto>”),ARCHIVO(“<objeto>”)]

Compara en el modo de Equalización el ARCHIVO especificado en el primer argumento con el ARCHIVO especificado en el segundo argumento y busca los elementos del primer archivo que existen y/o coinciden en el segundo archivo

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.8. Eliminar

Aplicar 2.

<OPERACION> -> ELIMINAR[<tipoObjeto>(“<objeto>”),<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> ELIMINAR[ARCHIVO(“<objeto>”),DIRECTORIO(“<objeto>”)]

Elimina un archivo de un directorio

Aplicar 8.

<OPERACION> -> ELIMINAR[DIRECTORIO(“<objeto>”),DIRECTORIO(“<objeto>”)]

Elimina un directorio dentro de una ruta

Aplicar 8.

<OPERACION> -> ELIMINAR[VALOR(“<objeto>”),CLAVE(“<objeto>”)]

Eliminar un valor dentro de una clave

Aplicar 8.

<OPERACION> -> ELIMINAR[CLAVE(“<objeto>”),CLAVE(“<objeto>”)]

Elimina una clave dentro de una ruta

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.4.9. Comando

Aplicar 3.

<OPERACION> -> COMANDO[<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> COMANDO[MENSAJE(“<objeto>”)]

Aplicar 10.

NOTA: El comando a ejecutar debe ser un comando válido dentro del entorno operativo, de lo contrario se retornará una excepción como comando no válido

---

4.4.10. Reportar

Aplicar 3.

<OPERACION> -> REPORTAR[<tipoObjeto>(“<objeto>”)]

Aplicar 8.

<OPERACION> -> REPORTAR[ARCHIVO(“<objeto>”)]

Aplicar 10.

<OPERACION> -> REPORTAR[ARCHIVO(“hpsReportes/reportes.rpt”)]

NOTA: Por defecto el Agente debe guardar todos sus reportes en el ARCHIVO "reportes.rpt" dentro de la carpeta "hpsReportes", pues en el intercambio de información este archivo se utiliza para actualizar la SIB del Gestor

---

4.4.11. Desplegar

Aplicar 2.

<OPERACION> -> DESPLEGAR[<tipoObjeto>("<objeto>"),<tipoObjeto>("<objeto>")]

Aplicar 8.

<OPERACION> -> DESPLEGAR[MENSAJE("<objeto>"),VALOR("<objeto>")]

Despliega un MENSAJE durante un tiempo equivalente a VALOR en milisegundos

Aplicar 8.

<OPERACION> -> DESPLEGAR[ARCHIVO("<objeto>"),VALOR("<objeto>")]

Despliega un ARCHIVO durante un tiempo equivalente a VALOR en milisegundos

Aplicar 10.

NOTA: Si el <objeto> especificado no corresponde a su <tipoObjeto> respectivo o no existe en el sistema, se retornará una excepción por incompatibilidad de tipo o por objeto no encontrado.

4.5. Sintaxis Para las Operaciones en Lps

4.5.1. Operación de Ejecución

Esta operación sirve para establecer una variable booleana que determina si las siguientes operaciones dentro del procedimiento se ejecutan o no.

EJECUTAR. Determina si las siguientes Operaciones dentro de un procedimiento se ejecutan o no, toma como argumento un tipo de objeto VAL y solo puede adquirir dos valores "**SI**" o "**NO**". La sintaxis es la siguiente:

EJECUTAR[VALOR("SI")]; // se ejecutan las siguientes operaciones
EJECUTAR[VALOR("NO")]; // no se ejecutan las siguientes operaciones

NOTA: Por seguridad de ejecución de cada procedimiento, se recomienda que cada uno de ellos inicie con una sentencia PLY con su valor "SI", con lo cual se reiniciará cada procedimiento en modo de ejecución, pues es posible que por operaciones anteriores o de otras políticas en ejecución paralela el valor de la variable de ejecución impida el desarrollo de un procedimiento que debería ejecutarse normalmente.

4.5.2. **Operación de Lectura**

Esta operación se utiliza para obtener la información de un objeto que puede ser un archivo, directorio, o una clave o valor del registro del sistema operativo. Si se conoce el objeto que se desea leer, se puede especificar el tipo de objeto mediante los siguientes especificadores

LEER. Se utiliza este operando para leer un objeto especificado en el primer parámetro y que se encuentra localizado en el objeto especificado en el segundo parámetro. Su resultado se guarda en un archivo de tipo temporal que se referencia a través de la variable RSL. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. La sintaxis es la siguiente:

LEER[tipoObj(“*objeto que se leerá*”),tipoObj(“*localización del objeto*”)];

A continuación se muestra un ejemplo de la sintaxis para leer el archivo “System.ini” del directorio “c:/Windows”.

LEER[ARCHIVO(“System.ini”),DIRECTORIO(“c:/Windows”)];

4.5.3. **Operación de Escritura**

Permite escribir un objeto en otro. La operación de escritura establece como objetivo un nuevo objeto, lo cual significa que si el objeto sobre el cual se desea escribir ya existe, el contenido será reemplazado por el nuevo objeto, lo que implica tener cuidado de no sobre-escribir archivos o valores cuyo contenido se necesita para la ejecución de una política. También se debe tener cuidad de sobre-escribir objetos que corresponden a claves o archivos que el sistema necesita para funcionar correctamente. La trama se describe a continuación.

ESCRIBIR. Operando que se utiliza para escribir el argumento del primer parámetro en el objeto especificado como argumento en el segundo parámetro. Los tipos que admite en el primer parámetro son: ARCHIVO, DIRECTORIO, REGISTRO, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, VALOR. La sintaxis es la siguiente:

ESCRIBIR[tipoObj(“*Contenido a escribir*”),tipoObj(“*Objeto sobre el cual se escribirá*”)];

Como el ejemplo se escribirá archivo “file.dat” en el directorio “c:\Archivos de Programa”.

ESCRIBIR[ARCHIVO(”file.dat”),DIRECTORIO(”c:\Archivos de Programa”)];

NOTA: Si el directorio especificado (o cualquier objeto) ya contenía alguna información u objeto, estos sería sobre-escritos, lo cual eliminaría contenidos anteriores.

4.5.4. **Operación de Adición**

Permite adicionar el contenido del objeto especificado en el primer parámetro en el contenido del objeto especificado en el segundo parámetro, sin alterar el contenido actual del objeto. La trama se describe a continuación.

ADICIONAR. Adiciona la información contenida en el primer objeto en el objeto especificado en el segundo parámetro. Cada objeto debe especificar su tipo. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. La sintaxis es la siguiente:

ADICIONAR[tipoObj(“*Obj que se adicionará*”),tipoObj(“*Objeto sobre el cual se realizará la adición*”)];

Para el ejemplo de análisis sobre la política de control de software una sentencia válida que se utilizaría para adicionar la información contenida en RSL en un archivo específico “INFRsw.dat” dentro del directorio “\infracciones” sería:

ADICIONAR[RESULTADO, ARCHIVO(“infracciones/INFRsw.dat”)];

NOTA: Cuando no se especifica el path[19], este se escribe en el directorio actual de la máquina virtual que estaría en la carpeta bin dentro del paquete jdk utilizado para cargar la máquina virtual, y se podría referenciar a dicho objeto solo con su nombre.

4.5.5. **Operación de Búsqueda**

Permite realizar la búsqueda de un objeto u objetos dentro de otro. El resultado de la búsqueda puede almacenarse en la variable RESULTADO y luego manipularse dentro de otra operación. La trama se describe a continuación.

BUSCAR. Esta operación realiza una búsqueda de un objeto especificado en el argumento del primer parámetro (también se puede rescatar una lista de objetos mediante el comodín asterisco <*> que rescataría todos los objetos) dentro del objeto especificado como argumento del segundo parámetro. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. La sintaxis es la siguiente:

BUSCAR[tipoObj(“*Objeto que se desea buscar”*),tipoObj(“*Objeto en el que se realiza la búsqueda”*)];

Una aplicación para el ejemplo de la política sobre software instalado que se utilizaría para buscar todos los objetos VALOR(“*”) dentro de una clave del registro que a su vez proporciona todas las subclaves y valores existentes recursivamente (CLAVE).

[19] Path: Ruta hacia un objeto

BUSCAR[VALOR("*"), CLAVE("RootKey.HKEY_LOCAL_MACHINE\\Software")**]**

NOTA: Las Ocurrencias al realizar la operación de búsqueda se almacenan de forma temporal en el objeto RESULTADO cuyo tipo es el mismo de la ocurrencia.

4.5.6. **Operación de Comparación**

Permite realizar la comparación de dos objetos del mismo tipo y su resultado puede rescatarse a través de la variable RESULTADO. La trama se describe a continuación.

COMPARAR. Esta operación compara el objeto especificado como argumento del primer parámetro con el objeto especificado como argumento del segundo parámetro. Las diferencias se describen de la forma: ***<Objeto 1> - <Objeto 2>***. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. La sintaxis es la siguiente:

COMPARAR[tipoObjeto("*Obj a comparar"*),tipoObj("*Obj de Referencia"*)];

Una aplicación como ejemplo para comparar dos archivos y su resultado adicionarlo en otro.

COMPARAR[ARCHIVO("c:\windows\localsw.dat"), ARCHIVO("c:\Archivos de Programa\SIBsw.dat")];
COMPARAR[RESULTADO, ARCHIVO("INFRsw.dat")];

4.5.7. **Operación de Equalización**

Permite realizar la comparación de dos objetos del mismo tipo y su resultado puede rescatarse a través de la variable RSL. La trama se describe a continuación.

EQUALIZAR. Esta operación compara el objeto especificado como argumento del primer parámetro con el objeto especificado como argumento del segundo parámetro. Y busca las ocurrencias de los elementos listados en ***<Objeto 1>*** que existen en ***<Objeto 2>***. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. La sintaxis es la siguiente:

EQUALIZAR[tipoObjeto(“*Obj a Equalizar”*),tipoObj(“*Obj de Referencia”*)];

Una aplicación como ejemplo para comparar dos archivos y su resultado adicionarlo en otro.

EQUALIZAR[ARCHIVO(“c:\windows\localsw.dat”), ARCHIVO(“c:\Archivosde Programa\SIBsw.dat”)];
ADICIONAR[RESULTADO, ARCHIVO(“INFRsw.dat”)];

4.5.8. **Operación de Despliegue**

Permite especificar la información que se debe desplegar en el momento que se realiza el control de la política y se utiliza sobre todo para notificar las infracciones que esté realizando el usuario respecto a las políticas implementadas. También puede usarse para realizar notificaciones de forma remota de alguna información que el administrador necesite dar a conocer de forma inmediata. La trama se describe a continuación.

DESPLEGAR. Despliega la información especificada, además de información que se desee hacer visible a través de la variable RESULTADO. Solo recibe parámetros de tipo MENSAJE o ARCHIVO en su primer argumento y un parámetro de tipo VALOR en su segundo argumento que define el tiempo que será visible este despliegue, el cual debe especificarse en milisegundos. La sintaxis es la siguiente:

DESPLEGAR[TipoObj(“*Aqui va la información o el Archivo que se desea desplegar”*),VAL(*“Tiempo visualización en milisegundos”*)];

Una aplicación para el ejemplo de la política sobre software instalado para visualizar la información cada vez que se realice una infracción.

DESPLEGAR[MENSAJE(“Infracción: el siguiente software se ha encontrado no está autorizado”), VALOR(“3500”)];
DESPLEGAR[ARCHIVO(“c:\infracciones\softwareInvalido.txt”), VALOR(“12000”)];

NOTA: El valor que se utilizará para contabilizar el tiempo de duración del despliegue de información debe especificarse en milisegundos.

4.5.9. **Operación de Eliminar**

Mediante esta operación se permite borrar un objeto contenido en otro. Esta operación debe especificarse con sumo cuidado para no afectar el sistema local o generar inconsistencias en su funcionamiento. La trama se describe a continuación.

ELIMINAR. Elimina el objeto especificado como argumento del primer parámetro que está localizado o contenido dentro del objeto especificado como argumento del segundo parámetro. Los tipos que admite en el primer parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. La sintaxis es la siguiente:

ELIMINAR[tipoObj(“*Obj que se desea eliminar”*),tipoObj(“*Obj donde está localizado el objeto que se desea eliminar”*)];

El siguiente ejemplo eliminar todos los valores que contengan la cadena playboy en su título de la clave donde se almacenan las direcciones almacenadas en el historial

ELIMINAR[VALOR(“*playboy*”),
CLAVE(“RootKey.HKEY_CURRENT_USER\\Software\\Internet Explorer\\TyperURLs”)];

4.5.10. **Operación de Ejecución de Comandos**

Mediante esta operación se permite la ejecución de un comando válido del sistema operativo.

COMANDO. Ejecuta el comando dentro del Objeto MENSAJE especificado como argumento del primer parámetro. La sintaxis es la siguiente:

COMANDO[MENSAJE(“*comando válido del Sistema Operativo”*)];

El siguiente ejemplo eliminar todos los archivos que contengan la cadena playboy en su título del directorio de archivos temporales de internet

COMANDO[MSG(“start c:/WINDOWS/Intern~1*playboy*”)];

4.5.11. **Operación de Importación**

Esta operación sirve para lograr la importación de un objeto desde el gestor hacia la localización dada en el equipo terminal.

IMPORTAR. Importa el objeto especificado como argumento del primer parámetro que está localizado en el Gestor y lo “copia” o ubica dentro del objeto especificado como argumento del segundo parámetro. Los tipos que admite en el primer parámetro son:

OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR, MENSAJE. Los tipos que admite en el segundo parámetro son: OBJETO, ARCHIVO, DIRECTORIO, REGISTRO, CLAVE, VALOR. La sintaxis es la siguiente:

IMPORTAR[tipoObj(“*Obj que se desea importar”*),tipoObj(“*Objeto donde será localizado el objeto que se desea importar”*)];

El siguiente ejemplo importar el archivo “systemHPS.ini” al directorio de archivos del sistema:

IMPORTAR[ARCHIVO(“systemHPS.ini”),DIRECTORIO(“c:/WINDOWS/System32”)];

4.5.12. **Procedimientos**

Los procedimientos contienen la información técnica y dinámica constituida por operaciones anteriormente descritas. Toda esta información permanecerá consignada en los archivos que constituyen la SIB tanto del gestor como del agente. Solo las operaciones especificadas dentro de los procedimientos se realizarán de forma repetitiva cada intervalo especificado en la variable Tiempo de Control (TMC). La trama se describe a continuación.

PROCEDIMIENTO. Define que la secuencia de segmentos a continuación, conforman una o varias instrucciones de control que representan las operaciones que cumple el propósito para el cual fue diseñada dicha política. Los procedimientos no asumen valores estáticos pues pueden variar según los requerimientos que el administrador desee implementar como control de dicha política y además puede estar compuesto por varios módulos funcionales que corresponden a operaciones específicas que relacionadas con las demás logran constituir de forma completa la implementación de la política de seguridad.

La sintaxis es la siguiente:

{OPR1;OPR2;...;OPRn;} // Procedimiento
{OPR1;OPR2;...,OPRn;} // Procedimiento

Donde:
OPR / Operación. Contiene la operación específica que define el control de la política que se está implementando. Está compuesta por una cantidad operadores de acciones puntuales con parámetros específicos como tipos de objetos o valores.

El siguiente ejemplo define un procedimiento de búsqueda de archivos que contengan la palabra “basura” en su nombre de archivo dentro del directorio “Internet Files” de la carpeta “WINDOWS”, escribe el resultado en la SIB del Agente, luego despliega un mensaje al usuario, borra los archivos encontrados en la carpeta. Luego en otro procedimiento despliega un nuevo mensaje de notificación al usuario.

```
{
  EJECUTAR[VALOR(“SI”)];
  BUSCAR[ARCHIVO(”*basura*”), DIRECTORIO(“c:/WINDOWS/Internet Files/”)];
  ESCRIBIR[RESULTADO,
    ARCHIVO(”c:/WINDOWS/System32/hegconPs/SIB.dat”)];
  DESPLEGAR[MENSAJE(“Los Sitios Web que está visitando no están autorizados
    y es una infracción que atenta contra la Seguridad de la Red de
    Datos”),VALOR(“4000”)];
  ELIMINAR[ARCHIVO(“*basura*”),DIRECTORIO(“c:/WINDOWS/Internet Files”)];
}
{
  EJECUTAR[VALOR(“SI”)];
  DESPLEGAR[MENSAJE(“Se ha denegado el acceso a estos Sitios Web”)];
}
```

En el ejemplo anterior, el primer procedimiento está compuesto por varias operaciones. Todo el procedimiento está contenido dentro de los signos **{ *//aquí adentro van las operaciones que constituyen el procedimiento* }**. Cada procedimiento está compuesto por ciertas acciones puntuales y que se desarrollan de forma secuencial. Para separar las operaciones se utiliza el signo (;) que identifica el fin de una operación.

Las acciones que componen la operación deben estar relacionadas con el signo (**;**) si su control se realiza sobre el mismo conjunto de datos o porción de información, lo que significa que si la acción anterior retorna un resultado, este resultado es almacenado para ser utilizado dentro de la siguiente acción (la que continúa al signo (**;**), este es un concepto similar al de almacenar un dato en un buffer).

Se recomienda que si se quiere definir una nueva acción cuyo control es de una naturaleza totalmente distinto de las acciones anteriores, entonces su sintaxis sea incluida en un nuevo procedimiento que contendrá una variable de tipo RESULTADO, que puede almacenar valores sin ser afectada por resultados obtenidos en operaciones anteriores (cada vez que se define un nuevo procedimento, RESULTADO se “resetea” para estar disponible para su uso en tiempo de ejecución). En la primera operación encontramos la acción BUSCAR el parámetro 1 ARCHIVO(“*basura*”) todos los elementos de tipo archivo que contengan el elemento String “basura”).

El uso de asterisco (*) es el mismo del comodín de DOS. La búsqueda debe realizarse en el elemento definido en el parámetro 2 que es un objeto de tipo DIRECTORIO que se encuentra en el path especificado (en el caso de este ejemplo la sintaxis es DIRECTORIO(”c:/WINDOWS/Internet Files/”).

El resultado es almacenado en la variable RESULTADO. Luego el resultado se escribe en el archivo “SIB.dat” que se encuentra en la ruta “c:/WINDOWS/Internet Files/”, y a su vez, dentro de la misma operación se despliega la información recolectada con otra especificada para efectos de notificación.

En la misma operación se procede a eliminar todos los objetos ARCHIVO que en su nombre contengan el String[20] "basura" del directorio especificado (que debe ser el mismo de donde se encontraron). En un nuevo procedimiento se despliega un mensaje que notifica que se procederá a restringir el acceso a dichos sitios web.

4.6. Implementación de Las Políticas de Seguridad en el Proyecto Hegcon-S

- **Política de Software Instalado en los equipos de la Red**

Primero se define el nombre de la política según su título

TTL= "Política de Control de Software Instalado en los Equipos de la Red"

También se define el Código para dicha política

COD= "1"

Se especifica el ente autor de la política

AUT= "Red de Datos Unicauca"

Se especifica el ente aprobador o autoridad que se encarga de validar la política

APR= "Vicerectoría de Investigaciones"

Se define la naturaleza de la política (CLS), en este ejemplo de orden educativo EDU

CLS= "EDU"

[20] String: Cadena de caracteres.

Se define las fechas de inicio y expiración o vigencia de la política (DTI y DTE)

DTI= ”2003-06-01”
DTE= ”2004-06-01”

Se define el nivel de seguridad o riesgo de esta política
RSK= ”MED”

Se define el tiempo de control(TMC) de la política (el valor debe ir especificado en milisegundos), en este caso el control se realizará cada 10 minutos

TMC=”600000”
INF. Definida anteriormente

Antes de especificar el procedimiento que se controlará de forma continua en el equipo, es necesario realizar una operación para posicionar la sib que controlará esta política. Esta operación no se realizará de forma continua, sino solo en el momento de la implementación de la política en el Agente.

En este caso la operación define que se escribirá (WRT) el archivo (FIL) llamado “SIBsw.dat” que contiene los datos que se desean controlar en el directorio (DIR) especificado en el path “c:\WINDOWS\System32\” que se considera un directorio vital para el sistema y por lo tanto no estará expuesto a malas manipulaciones por parte de los usuarios del equipo.

OPC=
IMPORTAR[ARCHIVO(”SIBsw.dat”), DIRECTORIO(”hpsFiles/sibsw.dat”)];

A continuación se determina el procedimiento que constituye la política descrito en **LPS (Lenguaje de Políticas de Seguridad).** Este procedimiento será controlado cada valor de tiempo especificado por TMC (que en caso específico de esta política es de 600000 o su equivalente de 10 minutos).

{
//policy2.lps Política de control del software instalado en este equipo
EJECUTAR[VALOR("SI")];
LEER[VALOR("*DisplayName"),CLAVE("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall")];
ESCRIBIR[RESULTADO,ARCHIVO("hpsFiles/sibLocal.dat")];
COMPARAR[ARCHIVO("hpsFiles/sibLocal.dat"),ARCHIVO("hpsFiles/sibsw.dat")];
ESCRIBIR[RESULTADO,ARCHIVO("hpsInfracciones/infr2.nfr")];
REPORTAR[ARCHIVO("hpsReportes/reportes.rpt")];
DESPLEGAR[MENSAJE("El siguiente software no Está Autorizado, por favor desinstalelo"),VALOR("6000")];
DESPLEGAR[ARCHIVO("hpsInfracciones/infr2.nfr"),VALOR("12000")];
}

A continuación se muestra el contenido técnico total de esta política en el momento de su implementación:

TTL= ”Política de Control de Software Instalado en los Equipos de la Red”
COD=”002”
STD=”ENB”
AUT= “Red de Datos Unicauca”
APR= “Vicerectoría de Investigaciones”
CLS= ”EDU”
DTI= ”2003-06-01”
DTE= ”2004-06-01”
RSK= ”MID”

TMC=”600000”

INF= ”Esta política establece de forma institucional que tipo de software esta autorizado por parte de la Administración de la Red de Datos para ser instalado en los equipos terminales de la Red. La infracción a esta política implicará una amenaza grave contra la seguridad de la Red y además puede provocar un funcionamiento incorrecto del sistema. “

Nota: “INF”, Se define de la misma forma para el resto de políticas implementadas

OPR=

IMPORTAR[ARCHIVO(”SIBsw.dat”), DIRECTORIO(”hpsFiles/sibsw.dat”)];

PRC=

{

//policy2.lps Política de control del software instalado en este equipo

EJECUTAR[VALOR("SI")];

LEER[VALOR("*DisplayName"),CLAVE("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall")];

ESCRIBIR[RESULTADO,ARCHIVO("hpsFiles/sibLocal.dat")];

COMPARAR[ARCHIVO("hpsFiles/sibLocal.dat"),ARCHIVO("hpsFiles/sibsw.dat")];

ESCRIBIR[RESULTADO,ARCHIVO("hpsInfracciones/infr2.nfr")];

REPORTAR[ARCHIVO("hpsReportes/reportes.rpt")];

DESPLEGAR[MENSAJE("El siguiente software no Está Autorizado, por favor desinstalelo"),VALOR("6000")];

DESPLEGAR[ARCHIVO("hpsInfracciones/infr2.nfr"),VALOR("12000")];

}

En este caso, además de visualizar el software que no debería estar instalado en los equipos terminales, esta política genera la siguiente salida:

Archivo hpsInfracciones/infr1.nfr:

DirectCD
IMesh
JBuilder 5 Enterprise
Teleport Pro
AutoCAD 2000 Uninstall
SnadBoy's Revelation v2
JBuilder 6 Enterprise
Cubis Gold
Starcraft Shareware(ED)
Doom Shareware for Windows 95
3ds max 4
LMS

Que corresponde a la lista del software que no debería estar instalado porque no se encuentra en la lista del archivo “hpsFiles/sibsw.dat”

Archivo hpsReportes/report1.rpt

gjuradoNKT
2003/11/5 3:53:13
INGENIERÍAS-3-329-CC1-3E-06-FF-DD-EE-C0-0A-B6
Política de Control de Software Instalado en los Equipos de la Red
---
gjuradoNKT
2003/11/5 4:3:13
INGENIERÍAS-3-329-CC1-3E-06-FF-DD-EE-C0-0A-B6
Política de Control de Software Instalado en los Equipos de la Red
---
gjuradoNKT
2003/11/5 4:13:14
INGENIERÍAS-3-329-CC1-3E-06-FF-DD-EE-C0-0A-B6
Política de Control de Software Instalado en los Equipos de la Red
---

Y este archivo se reportará a la base de datos del Gestor dando a conocer las infracciones ocurridas para la política de control de software instalado en los equipos de la Red, con el código del agente que realizó el control, el nombre de usuario que realizó la infracción y el momento en que se llevó a cabo el control.

De esta misma manera se implementarán dentro de la aplicación de una forma mas detallada cada una de las políticas piloto propuestas por este proyecto haciendo uso del **Lenguaje de Políticas de Seguridad (LPS).**

5. MÓDULO DE GESTIÓN. GESTOR

Corresponde a una Aplicación Software de mayor jerarquía instalado en la posición del Servidor[21] mediante el cual el Administrador de red puede gestionar las políticas de seguridad que se desean controlar por medio de los Agentes de Control.

5.1 Las Funciones Principales del Gestor

Adicionar, eliminar y modificar políticas; mantener la información correspondiente a Usuarios Responsables o encargados de llevar a cabo ciertas funciones de seguridad sobre la instalación y mantenimiento de los Agentes de Control en cada equipo terminal.

- Realizar operaciones de control sobre cualquiera de los Agentes.
- Verificar cuando un Agente ha sido instalado o desinstalado y realizar el procedimiento adecuado.
- Actualizar la **SIB** (Security Information Base) del Gestor con todos los eventos reportados en cada **SIB** de los Agentes (imagen).
- Intercambiar la llave pública del Gestor con cada uno de los Agentes y establecer conexiones seguras.
- Generar reportes dinámicos de acuerdo a las solicitudes del Administrador.

[21] Servidor: Equipo encargado de atender a los equipos que están como clientes.

En la figura 2. se describe el diagrama Conceptual del Sistema Hegcon-PS

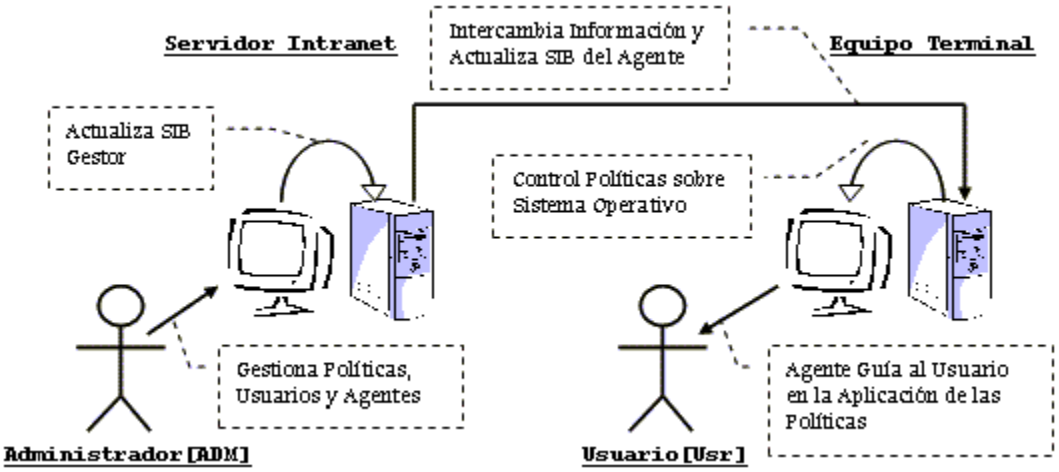

Figura 2. Diagrama Conceptual del Sistema Hegcon-PS

El administrador desde el gestor administra las políticas, en esta parte el administrador crea, modifica o borra las políticas que desea implementar mediante el pseudolenguaje, esta políticas son guardadas en la base de del gestor la cual es una SIB (Security Information Base).

El agente una vez instalado se conecta con el gestor, empezando de esta forma el intercambio de información entre estos. Primero el agente le envía al gestor los perfiles del equipo sobre el cual se ha instalado (dirección ip, dirección mac, la puerta de enlace, la dirección del dns, punto de red, oficina, datos del instalador, edificio, telefono).

Luego que el gestor registra toda la información anterior, le envía al gestor las políticas a que han sido implementadas, el agente las toma y actualiza su SIB, en ese momento inicia el proceso de control del agente. El gestor establece la hora y día en que el agente tendrá que enviar el informe de actividades del equipo

5.2 Diseño del Módulo de Gestión

El diseño del módulo de gestión que se muestra en la figura 3 pertenece al sistema **Hegcon-PS** está basado en la capacidad de prestación de datos ofrecida por conectividad a bases de datos de Java (**JDBC**)(2) sobre un gestor de bases de datos **MySQL(3)** configurado de forma segura (es obvio que una aplicación que pueda gestionar de forma remota los objetos de un sistema, y sean mal utilizados estos pueden llegar a ser altamente peligrosos), y la arquitectura de computación distribuida para realización de operaciones "On-Line" se basa en la arquitectura RMI.

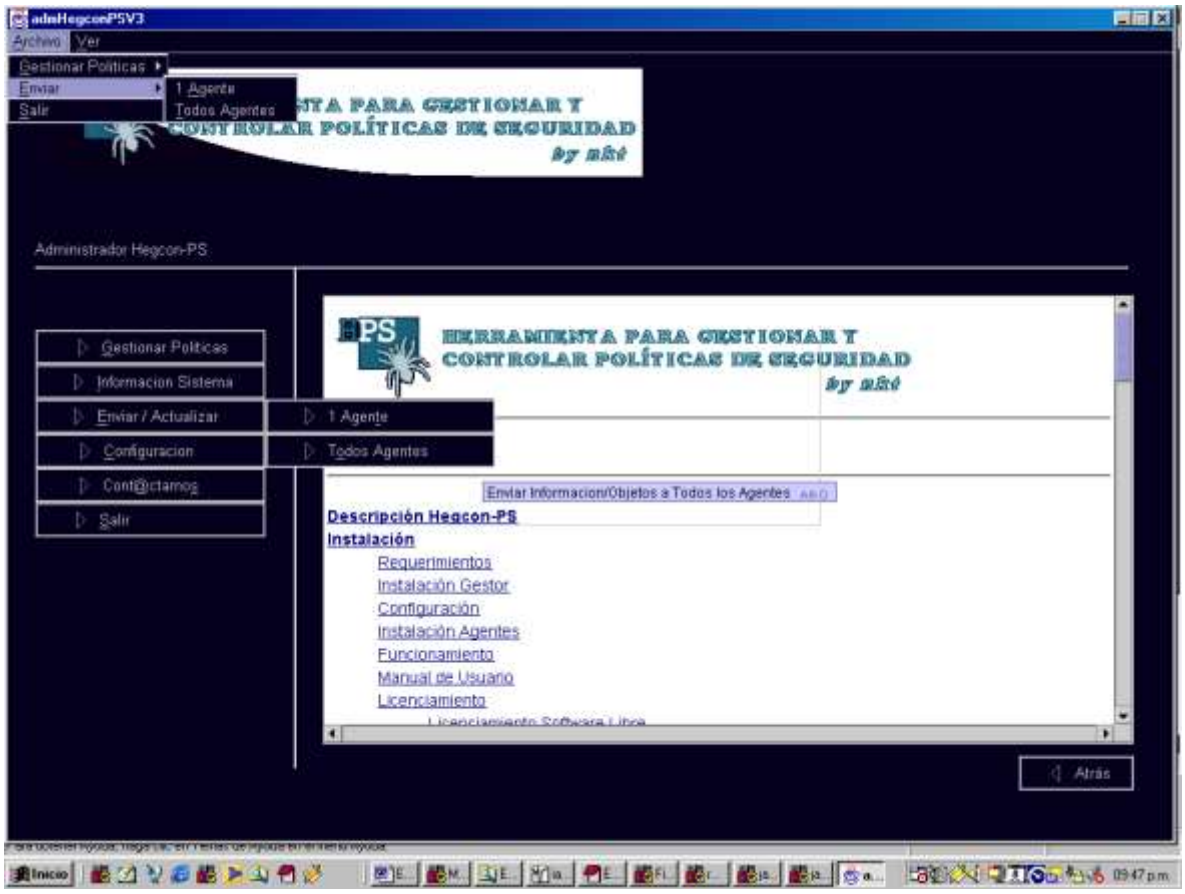

Figura 3. Interfaz de Administración del Gestor

5.3 Las funciones básicas del módulo de gestión son:

- Gestión de Agentes
- Gestión de Usuarios de los Servicios de Red
- Gestión de Políticas de Seguridad

A estas funciones se tiene acceso mediante la interfaz de administración del gestor que se muestra en la figura 3.

Además, el Gestor ofrece opciones de manejo de información como:

- Informes de Infracciones, Usuarios, Agentes, Políticas
- Reportes sobre la información de Infracciones, Usuarios, Agentes, Políticas.
- Edición manual de Archivos en equipos terminales

Dentro de las opciones de configuración se tiene:

- Configuración de Comunicación con Agentes
- Configuración de Apariencia
- Configuración de procesos de seguridad

Opciones de servicios como:

- Servicio de Mensajería
- Impresión Informes y reportes
- Envío de tareas para ejecución On-Line
- Ayuda html

5.4 Actividades de Gestión

5.4.1. Gestión de Agentes

Se tiene un registro de todos los agentes que se han instalado en la red, además de la información correspondiente a cada equipo terminal y datos anexos (ubicación física, codificación puntos de red). Además dentro de las opciones de configuración de agentes, se puede desactivar o reactivar un agente según alguna necesidad específica. La información correspondiente a actividades del agente también está registrada y puede ser manipulada a través del módulo de gestión en la opción Gestión Agentes.

Archivo > Gestionar > Agentes

O a través de la barra de herramientas sobre el botón de Opción

Gestionar > Agentes (doble click)

5.4.2. Gestión de Usuarios de los Servicios de Red

También se tiene un registro de todos los usuarios con cuenta dentro de la intranet, para poder ser identificados al momento de validarse en el inicio de sesión de los equipos terminales de red. Esta información permite identificar que usuario ha realización actividades que van en contra de las políticas implementadas.

Además, esta información está directamente relacionada con aquellos usuarios cuyas actividades dentro de algún equipo representen faltas contra el cumplimiento de las

políticas implementadas, lo cual permitirá al Administrador de Red tener el conocimiento exacto de las fuentes de eventos que ponen en riesgo la seguridad de la Red, además de realizar estudios de comportamiento por parte de los usuarios frente a los mecanismos de control implementados.

El acceso al módulo de gestión de usuarios es:

Archivo > Gestionar > Usuarios

O a través de la barra de herramientas sobre el botón de Opción

Gestionar > Usuarios (doble click)

5.4.3. Gestión de Políticas de Seguridad

Este sub-módulo de gestión permite realizar operaciones directas para crear, buscar, modificar, eliminar, obtener descripciones de las políticas de seguridad como se muestra en la figura 4.

La implementación puede ser específica de acuerdo al tipo de sistema operativo sobre el cual se desea ejecutar cada política (se pueden gestionar políticas específicas para win95, win98, winMillenium, winNT, win2000, winXP) aunque los propósitos de este proyecto se limitan a la ejecución de políticas sobre entornos win98

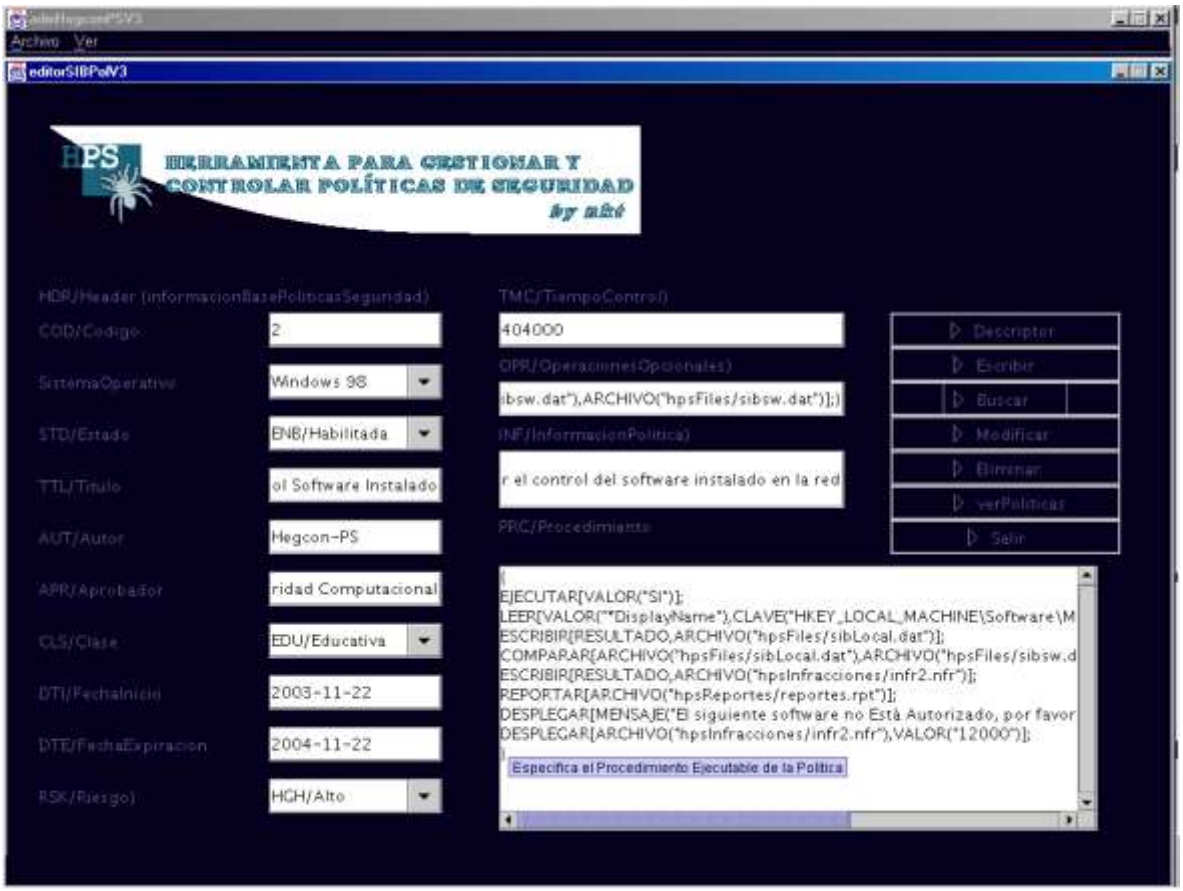

Figura 4. Módulo de Gestión de Políticas de Seguridad

Tenemos que en el proceso de creación de la política este permite visualizar las políticas de seguridad implementadas como se muestra en la figura 5.

Figura 5. Visualizador Políticas de Seguridad Implementadas

El gestor ofrece la oportunidad que el administrador visualize las operaciones que se van a llevar a cabo en el proceso de control como se muestra en la figura 6, donde se muestra el visualizador de políticas.

Figura 6. Descriptor de Políticas en LPS

El acceso al módulo de gestión de políticas es:

Archivo > Gestionar > Políticas

O a través de la barra de herramientas sobre el botón de Opción
Gestionar > Políticas (doble click)

5.4.4. Informes de Infracciones, Usuarios, Agentes, Políticas

El Administrador de Red requiere que el sistema brinde información de cada uno de los aspectos que se desean controlar como se muestra en la figura 7, lo cual implica el acceso a datos de forma globalizada y organizada.

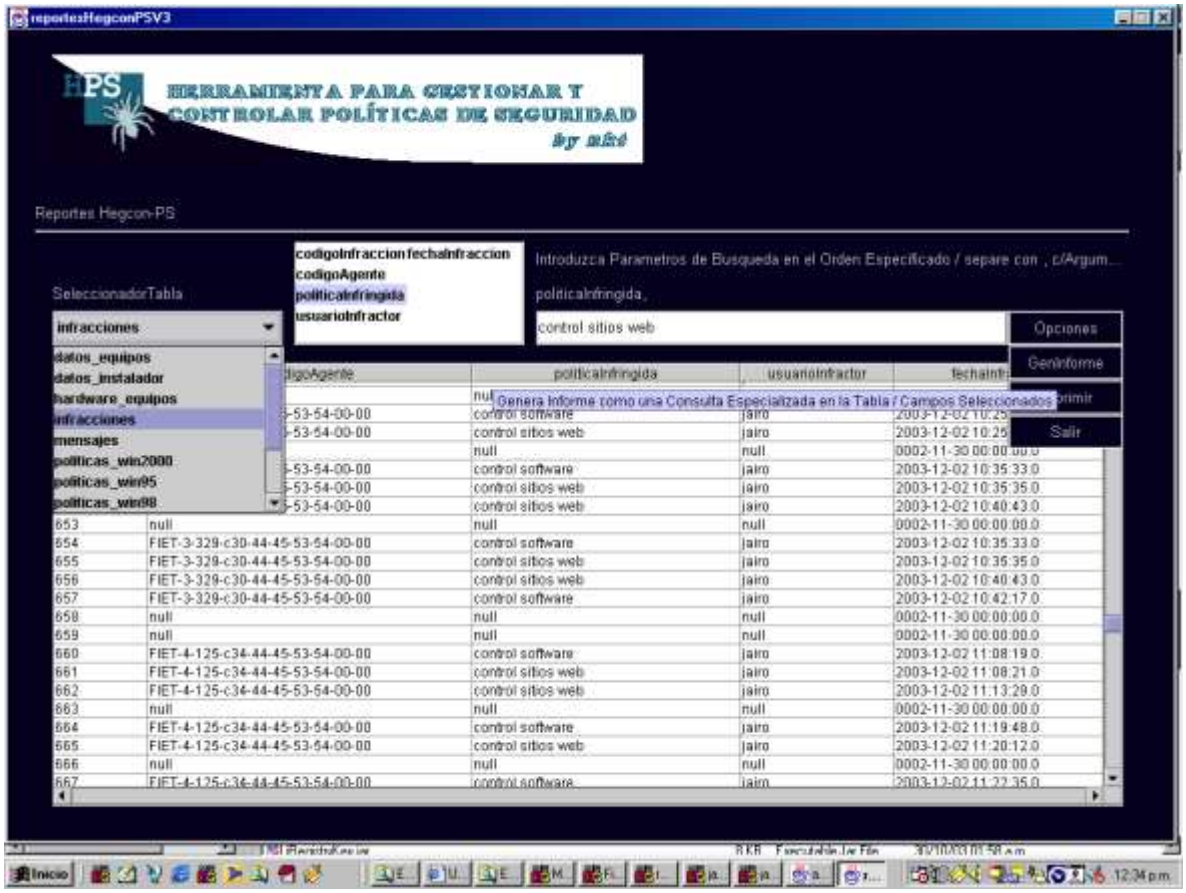

Figura 7. Informes y reportes del sistema Hegcon-PS

El Administrador puede decidir con total libertad que información desea visualizar.

El acceso al módulo de Informes es:

Ver > Informes > Infracciones
Ver > Informes > Agentes
Ver > Informes > Usuarios
Ver > Informes > Politicas

O a través de la barra de herramientas sobre el botón de Opción

Ver Informacion > Informes (doble click)

5.4.5. Edición manual de Archivos en equipos terminales

Permite la selección de un archivo específico como se muestra en la figura 8, para realizar su edición manual, lo cual puede ser de gran utilidad a la hora de realizar listas de parámetros de control, archivos de configuración, etc.

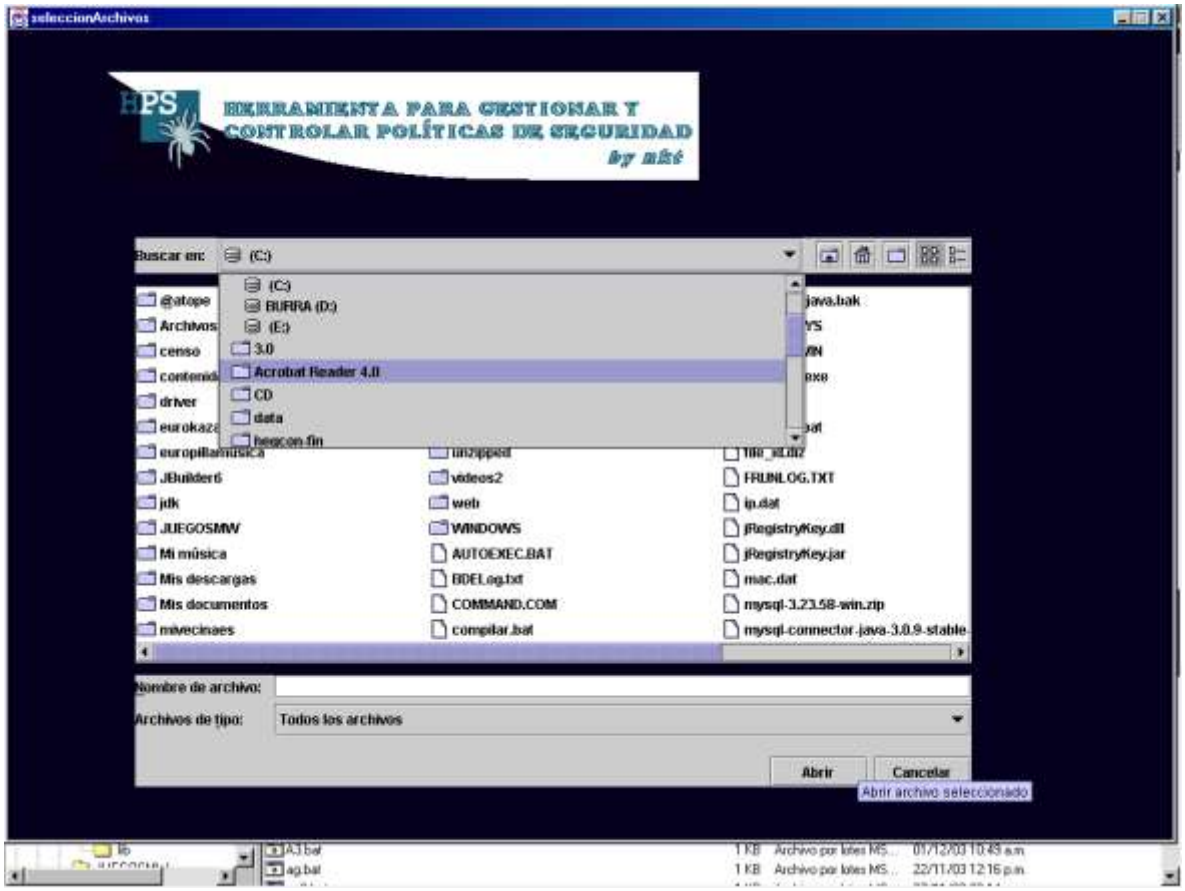

Figura 8. Proceso de edición manual de archivos

La secuencia de acciones es:

Archivo > Abrir

5.4.6. Configuración de Comunicación con Agentes

El módulo de configuración del sistema permite determinar el comportamiento del sistema frente a distintos aspectos relacionados con la comunicación como el tipo de acceso por parte de los agentes y el modelo de almacén de datos utilizado para soportar la SIB (Security Information Base) del Gestor, estos procesos se muestran en la figura 9.

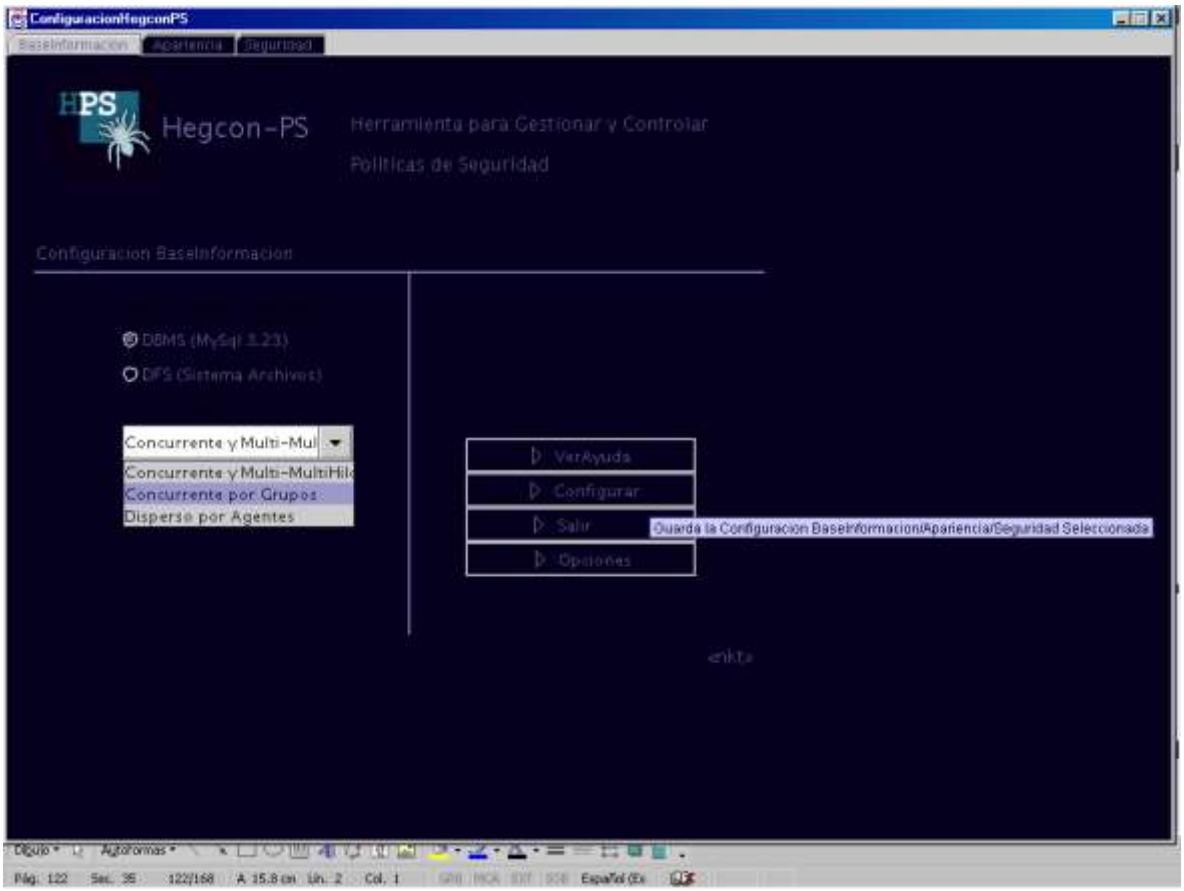

Figura 9. Definición de la configuración para la comunicación Gestor/Agente.

La secuencia de acciones es:

Ver > Configuración > BaseInformacion / Almacenamiento Datos/Accesos

Donde las opciones de selección para el almacén de datos son un sistema de archivos locales y difundidos a través de la arquitectura RMI o el sistema gestor de base de datos MySQL (para efectos de la implementación de este proyecto se trabajará con el DBMS MySQL 3.23).

5.4.7. Configuración de Apariencia

Esta opción de configuración permite al Administrador personalizar su paquete de software Hegcon-PS seleccionando desde un menú de opciones predeterminadas o añadiendo cada opción de presentación de forma manual como se muestra en la figura 10.

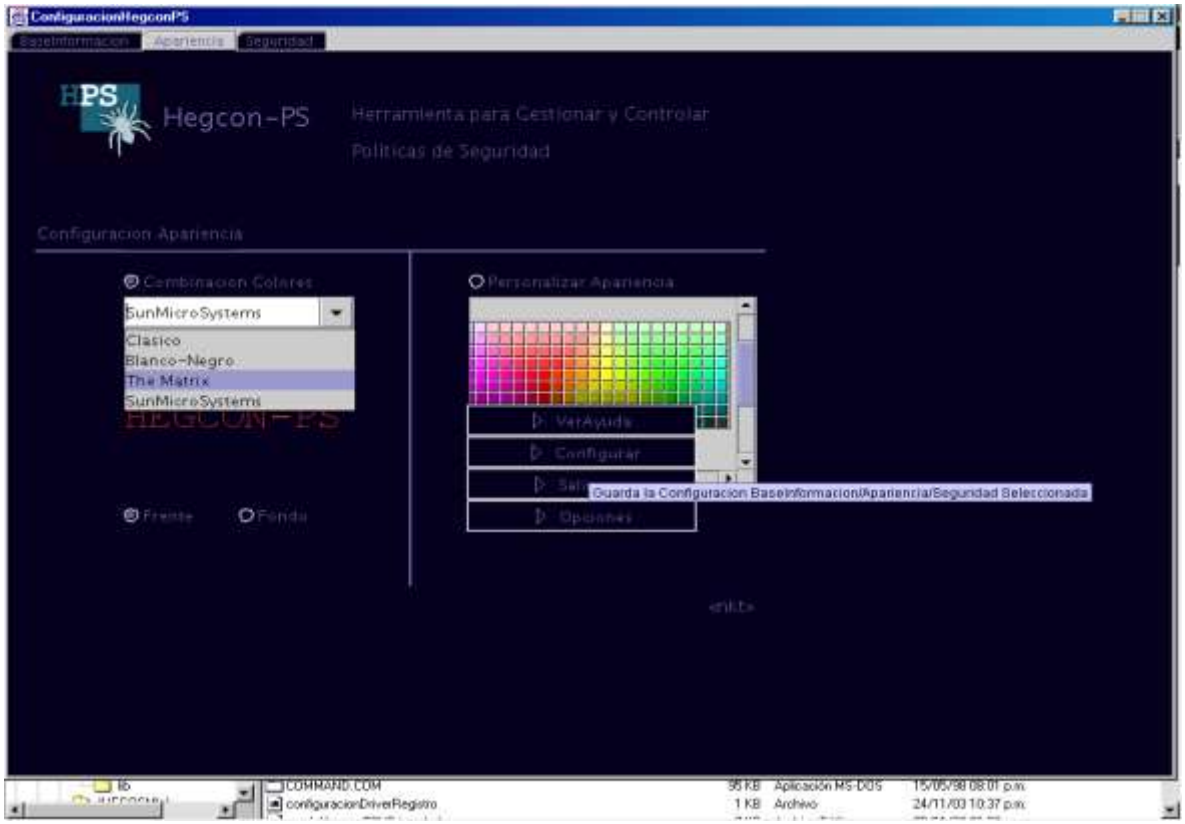

Figura 10. Personalización de la interfaz de Hegcon-PS

La secuencia de acciones es:

Ver > Configuración > Apariencia / CombinacionColores / PersonalizarApariencia

---

5.4.8. Configuración de procesos de seguridad

Así mismo el Administrador goza de la opción de configurar la seguridad como se muestra en la figura 11, con que el sistema realiza operaciones de intercambio de información y almacenamiento de datos, además de la opción de ejecución de algoritmo de puertos para establecer conexiones en ubicaciones distintas cada vez que se realice una nueva conexión, con lo cual se busca confundir las intenciones de posibles atacantes.

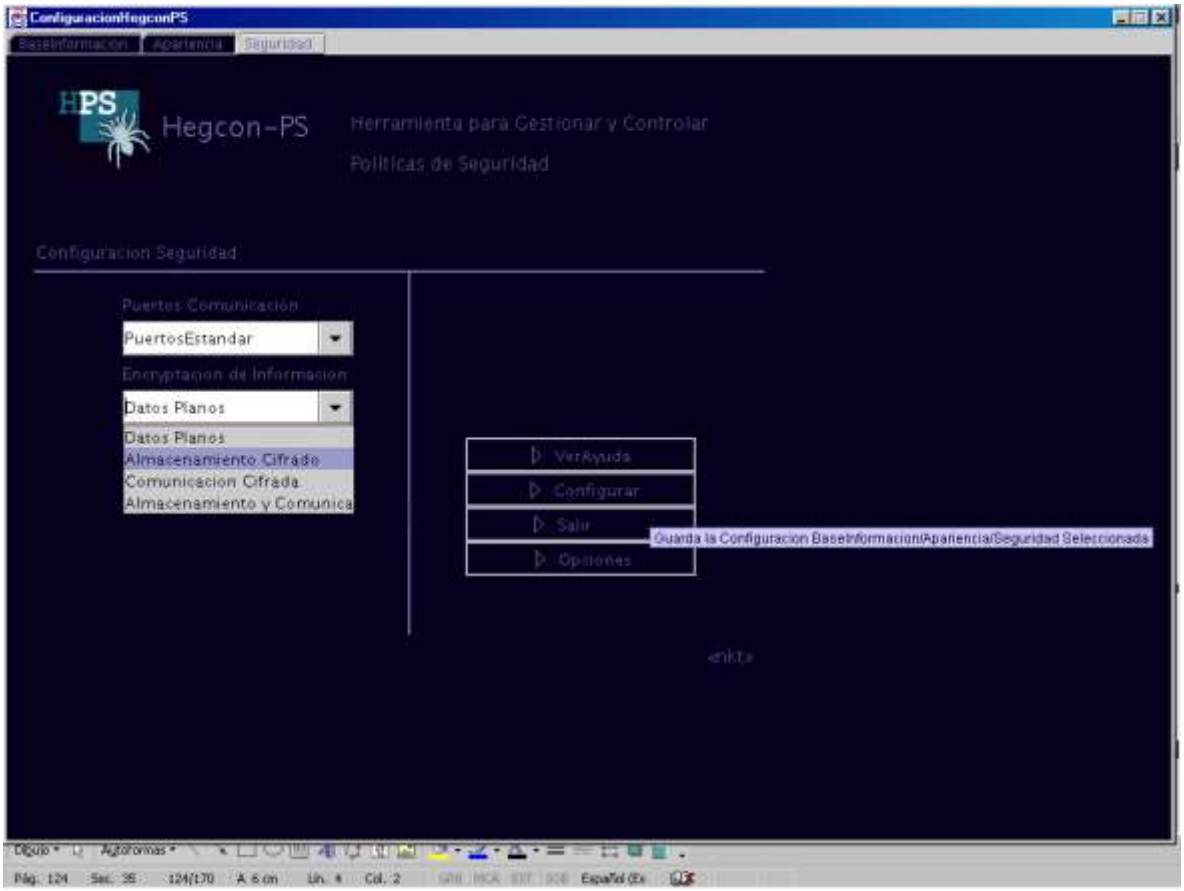

Figura 11. Opción de Configuración de la Seguridad

La secuencia de acciones es:

Ver > Configuración > Apariencia / Puertos Comunicación/Encriptación de Información

Donde Puertos de comunicación puede tomar los valores: Estandar o Algoritmo de Puertos, y Encriptación de Información puede ser: datos planos, Almacenamiento cifrado, comunicación cifrada, Almacenamiento y comunicación cifrados.

5.4.9. Servicio de Mensajería

Este servicio está estructurado sobre la arquitectura provista por RMI y mediante el cual el gestor tiene la posibilidad de transmitir mensajes de aviso, ejecución y tareas a los agentes de forma multicast[22] , por grupos e incluso a un agente en específico, todas estas operaciones se ejecutarán on-Line como se muestran en la figura 12.

[22] multicast: Envió de información a múltiples usuarios.

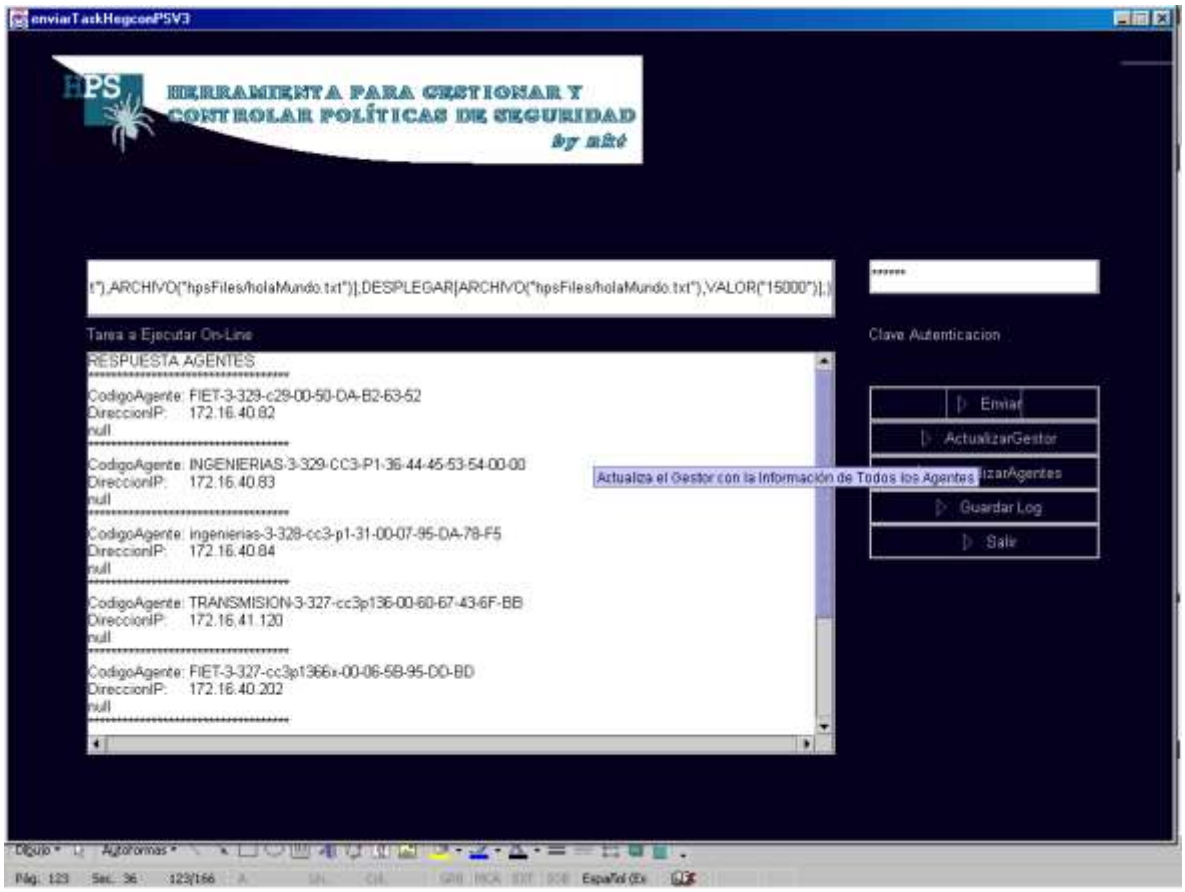

Figura 12. Envió de tareas On-Line

La secuencia de acciones es:

Archivo > Enviar > 1Agente
Archivo > Enviar > GrupoAgentes
Archivo > Enviar > TodosAgentes

O desde la barra de herramientas principal:

Enviar > 1Agente
Enviar > GrupoAgentes
Enviar > TodosAgentes

5.4.10. Impresión Informes y reportes

A través de estas opciones se busca lograr imprimir la información que el Administrador considere vital para llevar a cabo estrategias y planteamientos de seguridad en torno a la información recolectada a través del sistema Hegcon-PS.

.4.11. Ayuda html

Toda la información detallada del uso de este sistema se puede consultar a través de la misma ayuda que el sistema posee en formato html como se muestra en la figura 13, y que puede ser visualizado desde la misma aplicación o a través de un navegador web.

Figura 13. Ayuda de Hegcon-PS

Este módulo brinda todos los contenidos necesarios para guiar al administrador a explotar al 100% el sistema Hegcon-PS

la secuencia de acciones es:

Ayuda > Ver Ayuda

Como un servicio adicional, se brinda al Administrador contactar a los diseñadores y desarrolladores del sistema para resolver inquietudes vía web o encontrar respuesta en la página de soporte para el sistema **Hegcon-PS**

6. MODULO DE CONTROL. AGENTE

Corresponde a una Aplicación Software de menor jerarquía instalada en la posición de cada uno de los equipos que conforman la intranet y que está encargado de controlar las distintas políticas administradas a través del módulo de gestión, para lo cual su principal interacción es con el sistema operativo de cada equipo terminal de la red. para llevar a cabo el desarrollo piloto de este proyecto se determino trabajar sobre el entorno de Windows 98 considerado como la plataforma estándar de la mayoría de las redes Actuales y además este es el software licenciado por la universidad del cauca sitio donde se desea que implementen este producto software.

En desarrollos posteriores a este proyecto esta previsto se amplíe la aplicación a los otros tipos de entornos como Windows 95/NT/Me/2000/Xp, y Linux. El Agente corre de forma paralela con el sistema operativo como un Hilo o demonio, y además hace uso del registro del sistema operativo para llevar a cabo las correspondientes operaciones de control.

6.1. Funciones del Agente

Las funciones principales de los Agentes de Control serán:

- Actualizar la **SIB** (Security Information Base) del agente con todos los eventos y políticas infringidas.
- Cada agente intercambia su llave pública con el Gestor y establece conexiones seguras.
- Actualizar su propia **SIB** por cada operación del gestor.
- Desplegar mensajes informativos por cada una de las políticas infringidas y mostrar las sanciones pertinentes.

- Controlar de forma dinámica que se cumplan las políticas definidas por la administración de la red a través del módulo de gestión.

El agente consta de un interprete de código, el cual es quien recibe las instrucciones de las políticas por parte del gestor y se encarga de interpretarlas y asignar tareas especificas en el sistema de acuerdo a la política enviada por el gestor.

6.2. Operación del Agente.

La instalación de los agentes de control requiere la participación de alguien autorizado para realizar el respectivo registro y suministro de información en la etapa inicial de instalación. Esta información es vital ya que de allí en adelante se empezarán a desarrollar los respectivos perfiles de seguridad de usuarios cuya información será requerida por el administrador de red para realizar los respectivos planteamientos y estrategias de seguridad.

Cada vez que el sistema operativo arranca en un equipo terminal se carga en el sistema el Agente de Control de Políticas de Seguridad, el cual como primera instancia intenta establecer conexión con el con el Gestor, para tomar las políticas establecidas por el gestor y verifica si existen nuevas actualizaciones a las políticas anteriormente implementadas, o en caso de no existir estas políticas, realizar el respectivo intercambio de información.

En la figura 14 se muestra la interfaz de ejecución de una política cuando el agente se encuentra corriendo en un equipo.

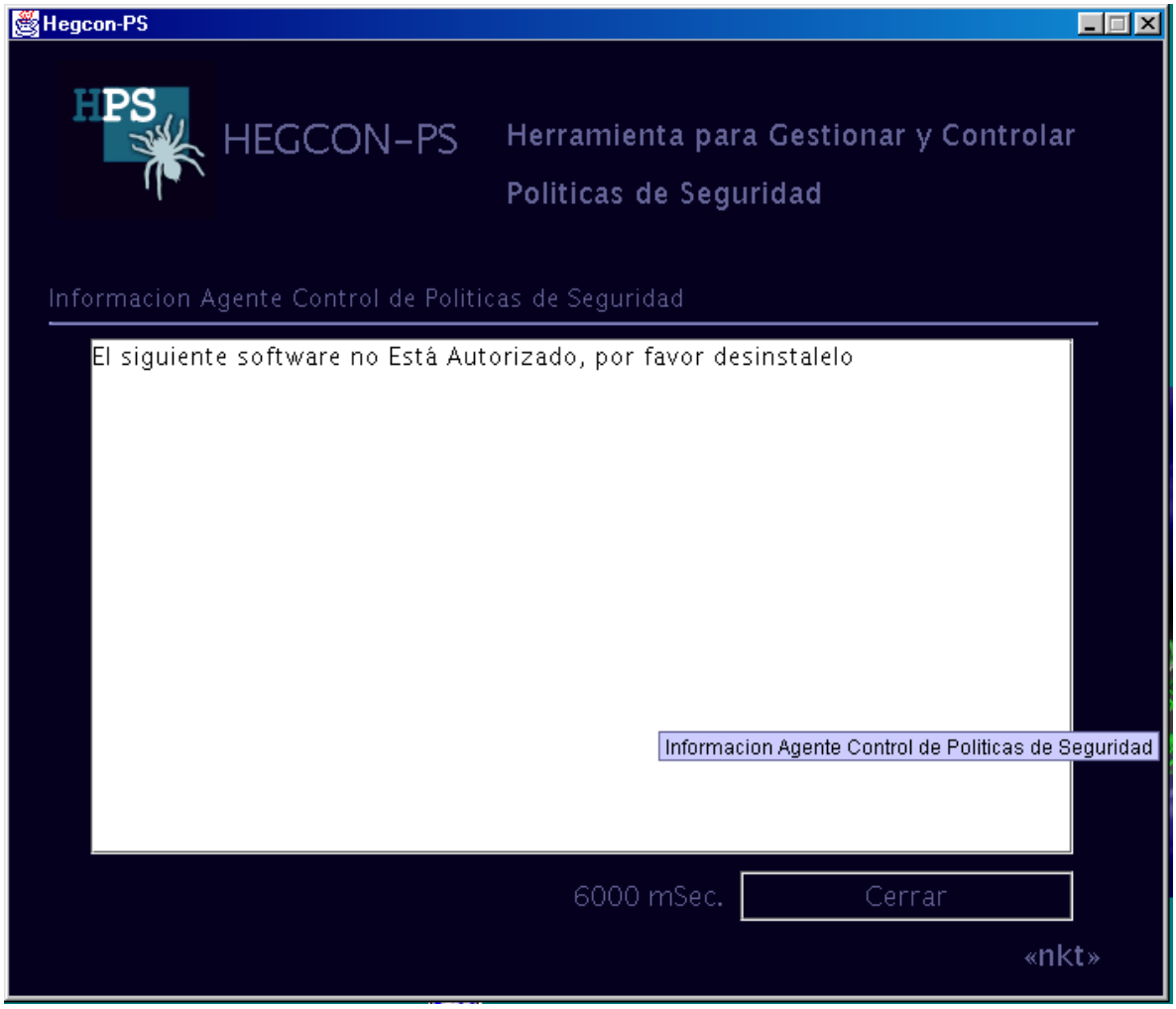

Figura 14. Interfaz de ejecución de una política.

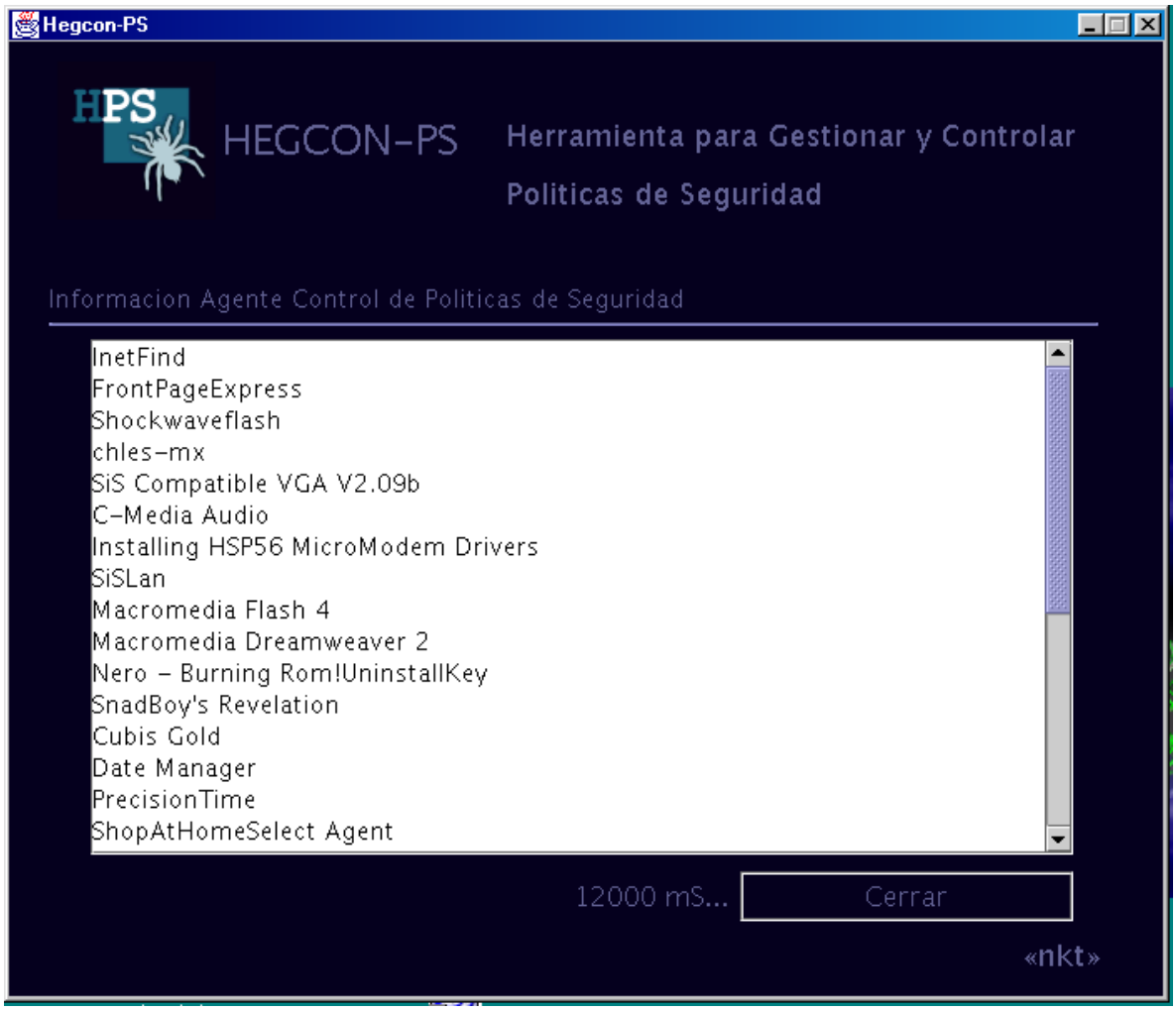

Figura 15. Interfaz de información al ejecutar la política control software.

En caso de existir reportes de infracciones como se muestra en el ejemplo de la figura15, (control software instalado), esta información es suministrada al gestor el cual la carga en la SIB, conociendo los datos del momento exacto en que se realizó la infracción, el usuario infractor y el agente que reportó la infracción.

Luego de realizadas las respectivas funciones de intercambio de información y actualización de su SIB, el agente procede a realizar el control de políticas de acuerdo a los códigos fuentes en **.lps.** [23]

Cada archivo **.lps** se carga como una tarea cuyo intervalo de ejecución se encuentra en el valor "timeControl"[24] dentro del correspondiente archivo infoPol.inf[25], es importante recordar que todos los datos de cabecera HDR explicados en el capítulo del **Lenguaje de Políticas de Seguridad (LPS)** se almacenarán en archivos de información infoPol.inf y que brindarán la correspondiente información técnica de la política implementada.

También es importante recordar que la información que se suministrará al Gestor como información de infracciones debe estar almacenada en el directorio correspondiente a los archivos report.rpt,[26] y que contiene la información correspondiente a el título de la política infringida, el usuario infractor, la fecha y hora, y el código del agente que reportó la falla.

La forma como generar un archivo report.rpt con información de infracciones se explicó en el capítulo de **Lenguaje de Políticas de Seguridad (LPS)**.

El funcionamiento y operación del Agente se basa en un analizador léxico-sintáctico que traduce las operaciones de alto nivel escritas en **LPS** ha operaciones primitivas sobre los objetos del sistema operativo (archivos y directorios) o del registro del sistema operativo (claves y valores del registro).

El mismo Agente sobre la máquina virtual de java se constituye en un entorno de ejecución a través del cual se realizan tareas de extracción de información y ejecución de operaciones, lo cual ordenado en torno a un aspecto específico puede servir para

[23] "Lps" Lenguaje de políticas de seguridad que encuentre en el respectivo directorio del banco de políticas.
[24] "timeControl". Control de tiempo.Tiempo de ejecución de la tarea
[25] infoPol.inf :Archivo que ofrece información sobre la política.
[26] report.rpt :Archivo que guarda los reportes generados por el agente.

administrar o controlar una actividad que no obligatoriamente tiene que ser el control de directivas de seguridad.

Debido a que el agente se basa en información contenida en el sistema, las políticas de seguridad no tienen estrictamente un orden restrictivo, si no mas bien reactivo, y debido a esto la naturaleza del proyecto se limita al aspecto educativo frente al uso de recursos y servicios por parte del usuario.

6.3. Configuración del Agente

El agente tiene dos modos de ejecución
java hpsAgente -s modo silencioso
java hpsAgente -v modo "verbose", información detallada de operaciones

En el modo silencioso el usuario no detecta que esta instalado un agente de control de políticas, ya que este solo captura la información del as infracciones generadas por el usuario dependiendo de las políticas implementadas y guarda esta formación en la SIB para luego ser enviada por el gestor. En este caso no se le despliega ningun tipo de mensaje al usuario en la pantalla al momento de la falta.

En el modo "Verbose"[27] como se muestra en la figura 16, el agente entrega al usuario información detallada sobre la operaciones no autorizadas que esta realizando en el equipo utilizado, desplegándole mensajes en la pantalla, en la cual se le informa de las faltas cometidas, de igual forma que en la configuración anterior guarda un reporte en su SIB y luego le es enviada al gestor de forma detallada.

[27] "Verbose" Muestra resultados de procesos al usuario. Traducción español**. Prolijo**: Cuidadoso, esmerado: están realizando un trabajo minucioso y prolijo para devolver al cuadro sus antiguos colores

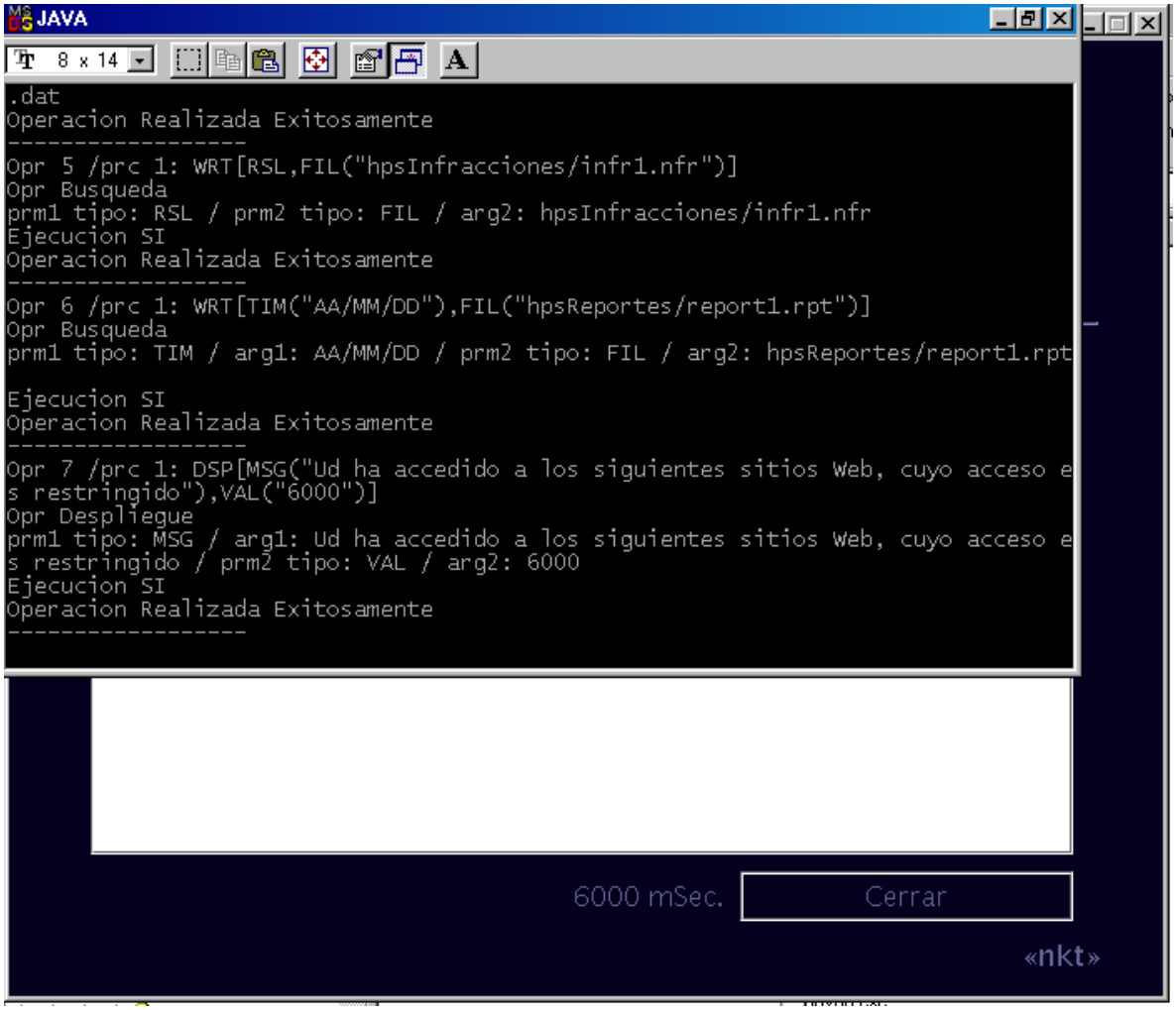

Figura 16. Ejecución del Agente en Modo Verbose

El agente puede ser administrado a través del módulo de gestión, el cual además de interferir sobre sus procesos, cancelando tareas, reactivando políticas, etc, puede llevar al agente a que de prioridades a funciones de control u operaciones que se consideren de extrema urgencia, y fuera de estas “arbitrariedades” el agente se limita a interpretar y ejecutar las tareas encomendadas a través del Lenguaje de Políticas de Seguridad, lo que implica que todas las operaciones deben ser expresadas en términos de LPS.

La información de modelamiento, diseño e implementación del Agente se encuentra, incluyendo las políticas de seguridad implementadas en LPS y la especificación del lenguaje se han estructurado de forma fácil de entender para el administrador. (Ver anexo C).

7. RESULTADOS

- Se logro desarrollar una Aplicación distribuida para gestionar y controlar Políticas de Seguridad dentro de la Red de Datos de la Universidad del Cauca mediante la cual se incremente el nivel de Seguridad de los servicios que la Red ofrece actualmente. La implementación del sistema evita al administrador de red la tarea de revisar presencialmente cada evento en cada equipo para identificar posibles fallos o malos usos de los servicios y recursos de red que podrían poner en juego la seguridad de la red.

- Se hizo análisis, diseño e implementación de modelo conceptual para generar políticas de seguridad que sirven como base para la generación de políticas de seguridad de una forma estructurada y especifica hacia los requerimientos o necesidades de la organización.

- Se logro definir la Sintaxis necesaria para llevar a cabo la transacción de directivas de seguridad y de información entre el Gestor y el Agente de tal manera que el control de Políticas de Seguridad se haga de forma dinámica. El Lenguaje de Políticas de Seguridad (LPS), brinda al sistema potencia y versatilidad al momento de implementar políticas de seguridad, además de ser un lenguaje de alto nivel lo cual facilita al administrador la tarea de desarrollar las directivas de seguridad.

- Se estableció bajo un patrón de clasificación específico las Políticas de orden técnico cuyo control se pueda llevar a cabo a través de los Agentes instalados en cada equipo de la Red. Estas políticas están limitadas a las operaciones o acciones que se pueden registrar en el sistema operativo de los equipos terminales. Además el control de estas políticas no es restrictivo, ya que se busca involucrar a los usuarios de la red en el correcto uso de los servicios y recursos de red, por lo cual se optó por enfocar el desarrollo del proyecto al aspecto netamente educativo.

- Se logro Implementar un sistema flexible a posteriores desarrollos según avance o evolucione la normatividad y políticas de administración que regularán la prestación de servicios por parte de la Red de Datos. Los desarrollos se pueden llevar a cabo tanto desde el punto de vista del comportamiento del sistema (recurriendo a nuevas implementaciones de políticas de seguridad a través del Lenguaje de Políticas de Seguridad LPS), o realizando nuevas implementaciones en el funcionamiento del sistema (redistribuyendo la lógica de la aplicación, o implementando nuevas funcionalidades en el sistema de gestión o de control).

- Se hizo un análisis de como la implantación de este proyecto puede facilitar las labores de administración y prestación de servicios, además de la reducción de costos que se derivan de las funciones de administración, operación y mantenimiento de la Red de Datos de la Universidad del Cauca.

CONCLUSIONES

Los estudios presentados en este documento son una alerta sobre el enorme trabajo que debe realizarse en la evangelización de conceptos sobre seguridad informática en la Universidad del Cauca. La única manera de evitar ser una víctima más de los ataques externos a través de redes globales, tales como Internet, es el conocimiento de las vulnerabilidades a que se está expuesto y el emprendimiento de acciones y estrategias para minimizar los riesgos.

El problema de la seguridad informática en la Universidad del Cauca cobra especial relevancia en vista del destacado papel que juega la interconexión de toda la red educativa y administrativa a Internet.

Como se puede ver existen varios y diversos métodos para implementar una red segura, pero ninguno por sí sólo puede brindarnos la suficiente seguridad, sino que es la combinación de todos estos elementos junto con una acertada planeación y control de políticas de seguridad, unos requerimientos específicos y las características propias de la red, son los que podrían ayudarnos a definir una eficiente estrategia de seguridad sin que todo esto interrumpa o entorpezca las actividades de los usuarios que son para los que finalmente se construyo la red.

Es necesario en todo sistema informático que se basa en la interacción Hombre-Máquina que los usuarios sean concientes del compromiso por parte de todos los actores y componentes del sistema, para lograr el uso óptimo y seguro de los programas y de la información. Estadísticas de seguridad no formales (datos obtenidos del “underground” o sub-mundo informático donde la cultura “hacker” se encarga de establecer o derribar los límites de seguridad de un sistema informático) anuncian y confirman que las fallas más grandes y vulnerabilidades más explotables (con sus respectivas consecuencias catastróficas) se originan en el mal uso de los usuarios por parte de los servicios y

recursos de red. Todo esto lleva a la idea de que “LA SEGURIDAD ES RESPONSABILIDAD DE TODOS”.

En futuros sistemas de protección de Redes existe la expectativa de la aplicación de procedimientos y metodologías propios de la Inteligencia Artificial (IA), con implementaciones complejas como sistemas de Agentes inteligentes, esquemas de procesamiento de información compleja, toma de decisiones, etc. La expectativa crece con la idea del desarrollo de un sistema capaz de decidir sobre sí mismo que actividades (por parte de usuarios u otros sistemas) pueden ser benéficas, inofensivas o perjudiciales y asumir la respuesta necesaria buscando mantener su “estado de bienestar”. Esto involucrará la gestión inteligente de procesos, desarrollo de perfiles de usuarios, “datawarehousing” de eventos y procesos complejos de computación forense. Hegcon-PS solo es un abrebocas de las implementaciones de alto nivel cuya expectativa crece día a día.

RECOMENDACIONES

Creación de las políticas de seguridad computacional para la universidad del cauca, teniendo en cuenta todos los aspectos organizacionales, legales y jurídicos que este proceso involucra.

Desarrollar, implementar, revisar y hacer cumplir las políticas de seguridad que satisfacen los objetivos de la universidad del cauca.

Desarrollar políticas que aborden las áreas de temas claves de seguridad, tales como la gestión de riesgos de seguridad, identificación de recursos críticos, seguridad física, gestión de sistemas y redes, autenticación y autorización, control de acceso, gestión de vulnerabilidades, gestión de incidentes, sensibilización, educación y privacidad.

Asegúrese que el propósito de cada política se refleje en estándares, procedimientos, prácticas, entrenamiento y las arquitecturas de seguridad que lo implementan.

Generar espacios de capacitación para los usuarios de la red de forma que estos puedan considerar la seguridad de la información como una parte normal de sus responsabilidades cotidianas.

Capacitar a los usuarios antes de entregarles una cuenta de correo, los usuarios deben recibir entrenamiento en los tópicos de la política de seguridad, tales como selección y protección de las contraseñas, permisos de accesos a archivos, expectativas de privacidad, navegación segura por Internet y la ingeniería social.

Una vez establecidas las políticas, los usuarios deben recibir entrenamiento en las consecuencias y sanciones derivadas de las violaciones a las políticas, incluso con sus posibles ramificaciones legales.

GLOSARIO

Agente. Corresponde a una Aplicación Software de menor jerarquía instalada en la posición de cada uno de los equipos que conforman la intranet y que está encargado de controlar las distintas políticas gestionadas a través del módulo de gestión o gestor.

Análisis heurístico*:* se trata de un análisis adicional que solamente algunos programas antivirus pueden realizar, para detectar virus que en ese momento son desconocidos.

Antivirus*:* son todos aquellos programas que permiten analizar memoria y unidades de disco en busca de virus . Una vez el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los archivos, directorios, o discos que hayan sido víctimas del virus.

Ataque: Ataque electrónico (típicamente no provocado) que intenta de alguna manera quebrar el sistema destino, los mecanismos de redes y de seguridad.

Auditorias: Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente

Autentificación: Método sistemático para establecer prueba de identidad entre dos o más entidades, normalmente usuario y host.

Atributos: los archivos y directorios tienen asignadas unas determinadas características que se denominan atributos. Estas pueden ser: sólo lectura, modificado, oculto, de sistema

Cadena*:* es una consecución de caracteres de texto, dígitos numéricos, signos de puntuación o espacios en blanco consecutivos. Alguna de las técnicas empleadas por los antivirus para la detección de virus es buscar determinadas cadenas de texto (o código) que éstos incluyen habitualmente.

Chat*:* se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo

Cifrado / Encriptado*:* es una de las características que, algunos de los virus existentes, utilizan para que los antivirus no los encuentren. Con ello, el virus se cifra, codifica o "encripta" automáticamente cuando realizar una infección. En cada infección realizará este cifrado de forma diferente, de tal forma que en cada ocasión sus cadenas o códigos son diferentes. El problema que el antivirus encuentra es que no siempre tiene que buscar los mismos códigos o cadenas de caracteres pues el virus en cada infección los hará diferentes.

Clave (*del Registro*): el Registro de Windows (Registry) es un elemento en el que se guardan las especificaciones de configuración del computador, mediante valores o claves. Estas claves cambiarán de valor, y/o se crearán, cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.

Cluster*:* con este término se identifica una sección física dentro de un disco de almacenamiento. Agrupa uno o varios sectores del disco que se encuentran consecutivos o adyacentes.

Desinfección*:* es la acción que realizan los programas antivirus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan la información infectada.

Debug*:* programa que permite la edición y creación de otros programas escritos en lenguajes como Ensamblador (no lenguajes de alto nivel). También hace posible la investigación del código interno en cualquier archivo.

El Gestor. Corresponde a una Aplicación Software de mayor jerarquía instalado en la posición del Servidor mediante el cual el Administrador de red puede gestionar las políticas de seguridad que se desean controlar por medio de los Agentes de Control.

Gusano*:* es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

In the wild*:* este término se refiere a una famosa lista en la que se reflejan los virus que, en la actualidad o en ese periodo de tiempo, se encuentran en su apogeo.

Infección*:* es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro computador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

Java*:* se trata de uno de los lenguajes de programación con el que se pueden crear páginas Web.

Macro / Virus de macro: una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo de, no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los archivos creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que

infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

Payload*:* tiene el significado de efectos secundarios que cualquier virus puede producir cuando ya ha pasado cierto tiempo desde el momento de la infección.

Polimorfico / polimorfismo*:* basándose en la técnica de auto encriptación, el virus se codifica o cifra de manera diferente en cada infección que realiza (su firma variará de una infección a otra). Si sólo fuese así estaríamos hablando de un virus que utiliza la encriptación, pero adicionalmente el virus cifrará también el modo (rutina o algoritmo) mediante el cual realiza el cifrado de su firma. Todo esto hace posible que el virus cree ejemplares de sí mismo diferentes de una infección a la siguiente, cambiando de "forma" en cada una de ellas. Para su detección, los programas antivirus emplean técnica de simulación de descifrado.

Pogramas (archivos .exe y .com): los archivos, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a 8) y una extensión que puede no existir o contener, hasta tres caracteres como máximo. Esta extensión especifica el tipo de archivo. Si es EXE o COM, el archivo será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones.

Registro de windows (registry*):* el denominado Registro de Windows (Registry) es un archivo en el cual se almacenan todos los valores de configuración e instalación de los programas que se encuentran instalados y de la propia definición del sistema operativo. Esta configuración se rige por claves, subclaves y valores que se pueden consultar y modificar y que la mayoría de programas modifican de forma automática (en algún aspecto) al instalarse.

Replica*:* se define como réplica la acción por la cual los virus se propagan o hacen copias de sí mismos, con el único objetivo de realizar posteriores infecciones.

Residente / virus residente*:* un virus que posea esta propiedad, será del tipo denominado "virus residente". Su característica es la de colocarse en secciones concretas de la memoria para, desde allí, atacar o infectar a todos los programas (archivos EXE o COM) que se ejecuten. El virus se instala en la memoria del computador y desde ella está continuamente comprobando si se ejecuta algún programa. Cuando esto ocurre, infecta el programa ejecutado.

Troyano*:* los troyanos no se pueden considerar virus ya que no se replican o no hacen copias de sí mismos. En realidad son programas que llegan a un computador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas y se instalan en nuestro computador. Al activarse puede dejar huecos en nuestro sistema, a través de los cuales se producen intrusiones.

Vacunación*:* mediante esta técnica, el programa antivirus almacena información sobre cada uno de los archivos. En caso de haberse detectado algún cambio entre la información guardada y la información actual del archivo, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones: Interna (la información se guarda dentro del propio archivo, de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio) y Externa (la información que guarda en un archivo especial y desde él se contrasta la información.

BIBLIOGRAFÍA Y REFERENCIAS

INTERNET

Nota: Por el continuo movimiento de las direcciones de Internet es posible que alguna de las enumeradas a continuación no se encuentren disponibles para consulta.

[1] MANUNTA, Giovanni. Presentación del libro Seguridad: una introducción. Consultor y Profesor de Seguridad de Cranfield University. Revista Virtual Seguridad Corporativa. http://www.seguridadcorporativa.org

[2] BORGHELLO F. Cristian. Tesis Doctoral. “Seguridad Informática: Sus implicancias e Implementación” 2001. http://www.cfbsoft.com.ar.

[3] AMADOR D. Siler, NIÑO Z. Miguel, FLECHAS Andres. Seguridad Computacional. Libro de consulta para administradores y usuarios. Popayán. 2001. http://www.kriptopolis.com.

[4] STERLIN Bruce. The Hacker Crakdown. Ley y desorden en la frontera electrónica. Austin.Texas. 1 enero 1994. http://www.kriptopolis.com.

[5] CARR, Jim. Thwarting Insider Attacks en NetworkMagazine. Vol 17. No 9. 96p. San Francisco. E.U. Editorial Calendar. Septiembre 2002. http://www.networkmagazine.com

[6] CONRY MURRAY Andrew. Securing End Users Fron Attack en NetworkMagazine. Vol 17. No 10. 88p. San Francisco. E.U. Editorial Calendar. Octubre 2002. http://www.networkmagazine.com

[7] TERRENCE W. Pratt, ZWLKOWITZ V. Marvin. Lenguaje de programación. Diseño e implementación. 3ª Edición. 2001.[]

[8] Documento DODD5200.28 Departamento de Defensa de los Estados Unidos de América.
http://www.lasalle.edu.co/csi_cursos/informatica/termino/seguridad_informatica.htm

[9] RICHAR Enrique Articulo:Virus informatico, desde el punto de vista biológico.
http://www.ubik.to/vr/vr16/virus.htm