UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMÁTICA"

Tema:

"Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY"

Trabajo de Graduación. Modalidad: **SEMINARIO de Graduación,** presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Pullutaxi Achachi William Leonardo

TUTOR: Ing. Clay Fernando Aldás Flores, Mg.

Ambato –Ecuador

Noviembre -2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema **"SISTEMAS MULTI-AGENTE PARA LA DETECCIÓN DE ATAQUES EN LOS ENTORNOS DINÁMICOS Y DISTRIBUIDOS DE LA EMPRESA IMPORTADORA REPCOPY "**, del señor William Leonardo Pullutaxi Achachi, estudiante de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Noviembre del 2012

EL TUTOR

Ing. Clay Fernando Aldás Flores, Mg.

AUTORÍA

El presente trabajo de investigación titulado **" SISTEMAS MULTI-AGENTE PARA LA DETECCIÓN DE ATAQUES EN LOS ENTORNOS DINÁMICOS Y DISTRIBUIDOS DE LA EMPRESA IMPORTADORA REPCOPY "**, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Noviembre del 2012

William Leonardo Pullutaxi Achachi

CC: 180415197-3

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes **Ing. David O. Guevara A. Mg.** e **Ing. Luis A. Solís S. M.Sc**, reviso y aprobó el Informe Final del trabajo de graduación titulado **" SISTEMAS MULTI-AGENTE PARA LA DETECCIÓN DE ATAQUES EN LOS ENTORNOS DINÁMICOS Y DISTRIBUIDOS DE LA EMPRESA IMPORTADORA REPCOPY"**, presentado por el señor William Leonardo Pullutaxi Achachi de acuerdo al Art. 18 del Reglamento de graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato

Ing. Oswaldo Paredes, M.Sc.
PRESIDENTE DEL TRIBUNAL

Ing. David O. Guevara A. Mg.
DOCENTE CALIFICADOR

Ing. Luis A. Solis. S. M.Sc.
DOCENTE CALIFICADOR

DEDICATORIA

A Dios por regalarme la vida, vida que estaba dedicada al estudio, empeño, sacrificio para salir adelante, cuidándome y dándome fortaleza para continuar, a mi familia quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en cada momento de logros y momentos difíciles, con sus consejos que hasta el día de hoy lo siguen haciendo.

A mis amigos/as que los conocí en el transcurso de mi vida estudiantil universitaria por haberme brindado una amistad incondicional, ayuda y sobre todo por estar junto a mí en los momentos más difíciles con sus consejos y palabras de apoyo.

William Leonardo Pullutaxi Achachi

AGRADECIMIENTO

*En primer lugar a **Dios** por darme la vida para lograr esta meta anhelada después de tantos esfuerzos y alegrías entre otras cosas, que he tenido durante mi formación profesional, me guiaste con tu luz por el camino correcto para no renunciar y por la felicidad que hasta el día de hoy tengo; en segundo lugar a cada uno de los que son parte de mi **familia** principalmente a mi Madre que día a día ha estado apoyándome con sus consejos abrazos, a mi padre, y a mi hermano mayor por su sacrificio, por su ayuda emocional y económica, a todos mis tios /tias, por siempre haberme brindado su fuerza y apoyo incondicional que me ha ayudado a llegar hasta donde estoy ahora.*

A la Universidad Técnica de Ambato en especial a la Facultad de Ingeniería en Sistemas Electrónica e Industrial, a cada uno de los docentes, los cuales me brindaron sus conocimientos y amistad.

William Leonardo Pullutaxi Achachi

ÍNDICE

CAPÍTULO I

EL PROBLEMA

CAPÍTULO II

MARCO TEÓRICO

CAPÍTULO III

MARCO METODOLÓGICO

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE DATOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

ANEXOS

Índice de Figuras

Índice de Tablas

RESUMEN EJECUTIVO

El presente trabajo denominado "SISTEMAS MULTI-AGENTE PARA LA DETECCIÓN DE ATAQUES EN LOS ENTORNOS DINÁMICOS Y DISTRIBUIDOS DE LA EMPRESA IMPORTADORA REPCOPY", mostrará el uso de tecnología de detección de ataques para ayudar a la Institución a tener un soporte sobre administración y monitoreo de la red.

La investigación realizada surge a raíz de la necesidad de proteger las vulnerabilidades de la red Empresarial, salvaguardando así la información que manejan dentro de ella. Sin embargo, la mayoría de las Empresas de alguna manera, no logran satisfacer sus necesidades sin un análisis técnico profesional, lo que ha generado pérdida de información. Como una solución, se realiza la implementación de Pandora FMS, lo cual permitirá mantener un control adecuado de lo que está sucediendo dentro de nuestra red.

Pandora FMS tiene como objetivo monitorear, evaluar de manera independiente todos los componentes de la red tales como: servidores, terminales y la red en sí. Además permitirá minimizar los riesgos que puedan surgir dentro de la Institución, para dar una garantía razonable de integridad, confidencialidad y disponibilidad de la información.

INTRODUCCIÓN

Al informe final del proyecto nominado "Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY" que se presenta a continuación, se le ha dividido en capítulos que pretenden facilitar la comprensión del contenido de este trabajo.

En el Capítulo I denominado "PROBLEMA", consta de; tema, planteamiento del problema, contextualización, análisis crítico, prognosis, formulación del problema, delimitación del objetivo de investigación, justificación, objetivo general y objetivos específicos.

En el Capítulo II denominado "MARCO TEÓRICO", se establece el marco teórico en el cual se va a trabajar, con sus antecedentes investigativos, fundamentación legal, hipótesis y el señalamiento de las variables de la hipótesis.

En el Capítulo III denominado "METODOLOGÍA", se determina la metodología de investigación a utilizar, enfoque, modalidad básica de la investigación, tipo de investigación, población.

En el Capítulo IV denominado "ANÁLISIS E INTERPRETACIÓN DE RESULTADOS", se tabula los datos obtenidos de la encuesta aplicada a la Empresa para su posterior análisis e interpretación de resultados y la verificación de la hipótesis.

En el Capítulo V denominado "CONCLUSIONES Y RECOMENDACIONES", en este capítulo se presenta las conclusiones obtenidas después del análisis de la información recolectada de la encuesta para luego proponer las recomendaciones necesarias a cada una de ellas.

En el Capítulo VI denominado "PROPUESTA", se presenta el estudio de la herramienta estudiada e implantada en la Empresa para monitorear los incidentes de la red.

Y por último se ubican los anexos en los cuales encontramos los documentos recolectados en libros y la Web como fuente de información, entre estos la encuesta.

CAPÍTULO I

EL PROBLEMA

1.1.Tema

Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa “Importadora REPCOPY”

1.2.Planteamiento del problema

1.2.1. Contextualización

La seguridad informática a nivel mundial está tomando mucha importancia, debido al alto índice de ataques a los sistemas informáticos, como a las redes de datos, dejando como resultado pérdidas económicas cuantiosas, y la mala manipulación de la información por parte de los intrusos, poniendo en evidencia datos confidenciales de uso exclusivo de la persona o Institución.

En la actualidad la seguridad de la información de cualquier Empresa, es un punto muy importante para el éxito de la misma, pues de dicha seguridad, es de donde más dependen todas sus fortalezas y al mismo tiempo sus debilidades. Todas las acciones realizadas dentro de un ente son importantes para el crecimiento del mismo, pero como bien sabemos la seguridad de datos depende del administrador de sistemas, es

decir el objetivo de la seguridad será mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por la computadora.

Es por ello que el factor humano ha tomado cada vez más, un papel y posición muy importantes dentro del control de seguridad de la información de la Empresa, con el fin de que la información manejada dentro de la Empresa sea óptima y tenga un alto grado de confiabilidad.

La mayoría de los Empresas en el país cuentan con los sistemas informáticos distribuidos los mismos que permiten a los empleados el ahorro de tiempo al momento de enviar y recibir información, pero su uso no garantiza que la información obtenida sea la correcta, es decir que durante el proceso de intercambio de datos estos pudieron haber sido víctimas de programas o personas que quieren perjudicar a la Empresa, mediante el robo, la modificación o el ataque a las redes de datos causando pérdidas económicas y el desprestigio como Institución.

En el Ecuador hoy en día hablar de fraudes informáticos, ataques a las redes de datos o ser víctima de hackers, crackers, malware no es un tema nuevo, esto es un problema que viene creciendo frecuentemente, el problema radica en que los administradores de las bases de datos o redes de comunicación nos preocupamos por mantener las redes en buen estado o que la comunicación se lleve a cabo correctamente, o que las bases de datos funciones normalmente, pero el problema principal es que no nos preocupamos por la seguridad de la información, dando así libertad a los delincuentes informáticos a que se introduzcan a nuestros sistemas, y a la red por donde viaja la información, ocasionando así pérdida, robo, modificación de la información, y dejamos un lado las reglas de la seguridad informática que es mantener la integridad, confidencialidad y disponibilidad de la información.

En Tungurahua en la Empresa Importadora REPCOPY tampoco tiene políticas de seguridad, es por esto que hace de la red muy vulnerable y fácil de acceder para cualquier persona, dando así riendas sueltas para el robo de la información y la mala manipulación del mismo, provocando así el malestar en el personal administrativo de

la Institución, es por esto que hace necesario realizar un estudio de nuevas técnicas de detección de intrusos como es los sistemas Multi-Agente en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY.

1.2.2. Análisis crítico

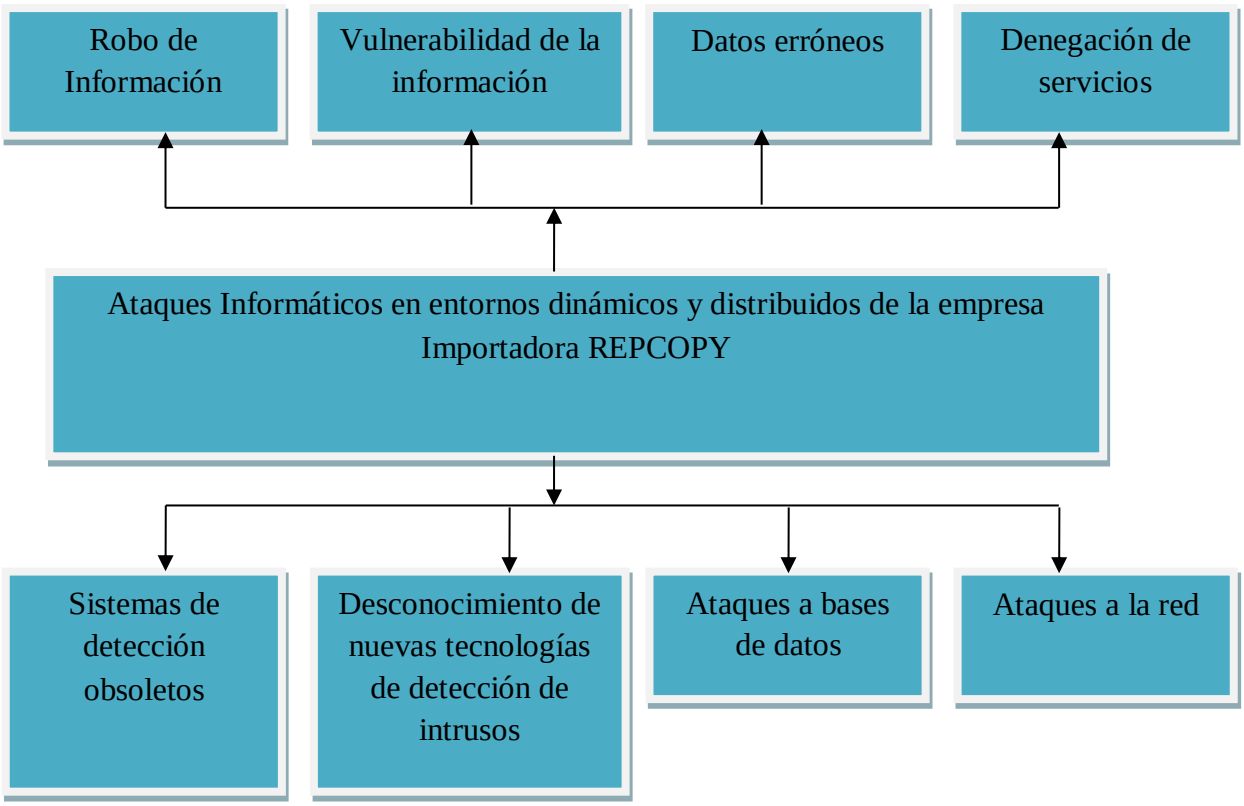


Figura 1: Árbol del Problema

Autor: William Pullutaxi

La tecnología informática avanza constante mente, por la cual hace imprescindible el estudio diario de nuevas herramientas que aparecen día a día y más aún cuando de proteger información de vital importancia para una Empresa se trata.

En la Empresa Importadora REPCOPY se preocupan solamente de la infraestructura de la red y que las bases de datos trabajen correctamente, dejando un lado la seguridad de las mismas, o a su vez utilizando técnicas o herramientas obsoletos de

protección haciendo de esto muy vulnerable ante cualquier ataque o delincuente informático que roba la información y hace uso de las mismas con el fin de perjudicar a la Institución.

El estar desactualizado o el desconocimiento de las herramientas avanzadas de detección de intrusos es otra detonante para que la información que viaja por la red de la Empresa sea vulnerable y fácil de acceder perjudicando económicamente a la Empresa.

Las herramientas de protección utilizadas actualmente por la Empresa permiten que los delincuentes informáticos actúen fácilmente y ocasionen ataques a las bases de datos y a la red, generando datos erróneos y también provoquen la interrupción de la misma que producen retardos en las actividades diarias, pérdida de tiempo, y sobre todo robo de la información.

La protección de la información es de vital importancia y un punto clave para el crecimiento de la misma es por esto que debemos actualizarnos diariamente y hacer uso de herramientas que mejoren la seguridad de la información.

1.2.3. Prognosis

La importadora de REPCOPY tendría que afrontar problemas por el robo y a la mala manipulación de información por personas ajenas y la inconformidad de las autoridades por la falta de control en el acceso a la información que aquí manejan, lo que daría paso al desprestigio de la Institución, reduciendo el desarrollo corporativo de la misma.

Tecnológicamente la Institución contaría con herramientas para controlar la inseguridad pero no las suficientes y necesarias para mantener total integridad y confidencialidad en las redes de datos.

Por lo que se hace necesario el estudio de los "Sistemas MULTI-AGENTE para la detección de intrusos en entornos dinámicos y distribuidos"

1.2.4. Formulación del problema

¿Cómo incide un Sistema MULTI-AGENTE en la detección de ataques en sistemas dinámicos y distribuidos de la Empresa Importadora REPCOPY"?

1.2.5. Preguntas directrices

¿Cuáles son los ataques informáticos más frecuentes que sufre la Empresa Importadora REPCOPY?

¿Qué características posen los entornos dinámicos y distribuidos que maneja la Empresa Importadora REPCOPY?

¿Qué herramientas será la más apropiada para evitar los ataques informáticos a entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY?

1.2.6. Delimitación del problema

Teórico:

- Campo: Seguridad Informática
- Área: Fraudes Informáticos
- Aspecto: Entorno dinámicos y distribuidos

Tiempo:

Para el presente trabajo investigativo estará enmarcado durante seis meses desde su aprobación.

Espacio:

La presente investigación se llevará a cabo en la Empresa REPCOPY.

1.3.Justificación

La implantación de un sistema de detección de ataques en la red permitirá aplicar las bases teóricos prácticos adquiridos en el transcurso de la carrera universitaria, la misma que busca la especialización en el campo de desarrollo, la misma que permitirá fomentar la creatividad y actitud, todo esto permitiendo el crecimiento personal y profesional de cada estudiante abriendo así caminos para el crecimiento y la excelencia.

El estudio de los sistemas Multi-Agente para la detección de intrusos se lo realiza principalmente enfocado a mantener un control adecuado de la información en la red de la Empresa.

El desarrollo del Proyecto será de gran utilidad para mejorar el control de intrusos, evitar el robo de información y la mala manipulación de la misma, así como datos incorrectos al momento de enviar y recibir la información, brindando así datos seguros y confiables.

Debido a la gran información de uso confidencial para la Empresa, se torna de gran utilidad el realizar el estudio de los ataques informáticos que día a día crese constantemente, ya que sería de gran aporte tanto para la Institución como para el personal que forma parte de ella, ya que con ello el investigador estará en la capacidad de averiguar las principales errores de seguridad y buscar una posible solución de manera inmediata.

El Proyecto es factible de realizar porque se cuenta con la información necesaria que proporcionará la Empresa, existe personal especializado en la FISEI para guiar el

desarrollo del trabajo, así como también libros necesarios que se encuentran en la biblioteca de la Facultad y en la Web.

1.4.Objetivos

1.4.1. Objetivo general

Implantar un sistema MULTI-AGENTE para reducir los ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY

1.4.2. Objetivos específicos

- Analizar los posibles ataques informáticos en los diferentes entornos en la Empresa Importadora REPCOPY.
- Analizar las características actuales de los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY.
- Proponer una herramienta Multi-Agente como solución ante ataques en entornos dinámicos y distribuidos.

CAPÍTULO II

MARCO TEÓRICO

2.1.Antecedentes investigativos

Una vez planteada el problema se procedió a recolectar información relacionada que permitirá dar soluciones óptimas y viables al mismo. Para ello se visitó la biblioteca central y de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato con el fin de recolectar información referente al presente tema o similares.

Lamentablemente no se pudo obtener información puesto que en la biblioteca no hay ningún trabajo de investigación referente al presente tema.

Luego se procedió a investigar en la Web, logrando obtener trabajos referentes al tema de investigación obteniendo gran información de ayuda para el desarrollo del proyecto de sistemas multi-agente para la detección de ataques en entornos dinámicos y distribuidos.

En el año 2001 Borghello Cristian Fabián elaboró una tesis de licenciatura en sistemas con el título "Seguridad Informática sus implicancias e implementación"

En el año 2005 el Ing. Wilson Eduardo Sotomonte Nieto elaboro una tesis de Magíster en Ingeniería en Automatización Industrial con el título "Estrategias de sistemas de agentes (simple y múltiples): caso de estudio fútbol de robots"

De estos trabajos se tomarán como referencia las siguientes conclusiones:

Al implementar técnicas de seguridad en bases de datos garantizará la integridad de los datos, dando así mayor confianza a la hora de obtener consultas y reportes.

La correcta utilización de los recursos tecnológicos en este proyecto informático permitirá asegurar toda la información para que no sea víctima de intrusos.

2.2.Fundamentación legal

Constitución de la República del Ecuador

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumakkawsay.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

Sección novena
Gestión del riesgo

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Realizar y coordinar las acciones necesarias para reducir vulnerabilidades y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
5. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

2.3.Fundamentación teórica

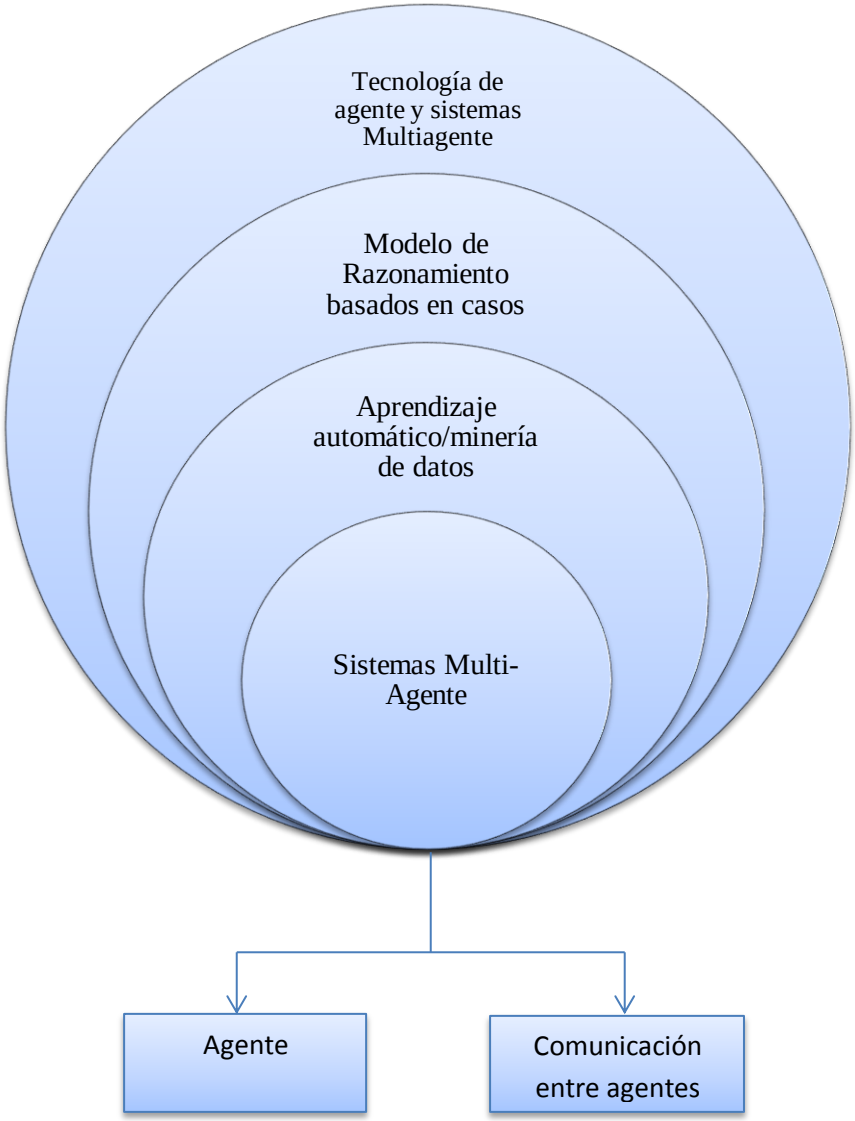


Figura 2: Variable Independiente

Autor: William Pullutaxi

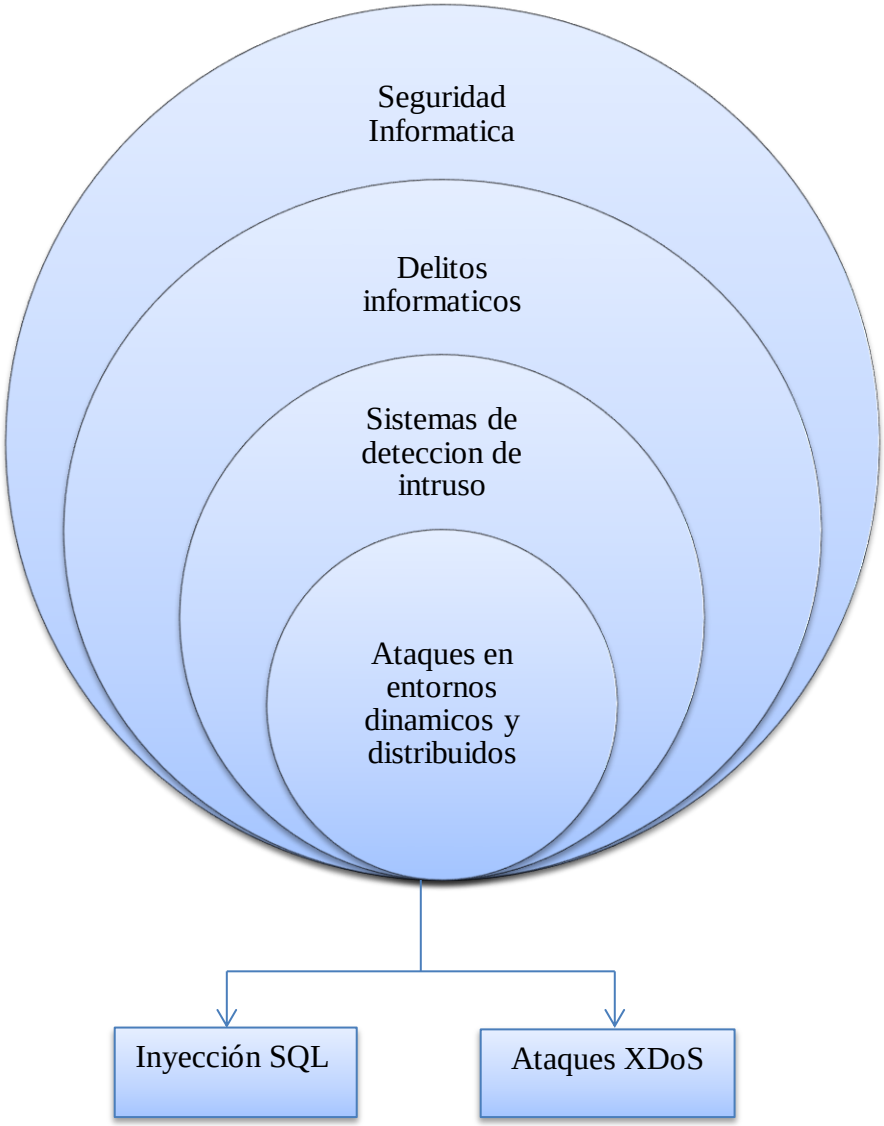


Figura 3 : Variable dependiente

Autor: William Pullutaxi

2.3.1. Tecnología de agente y sistemas multiagente

Para el Doctor Cristian Pinzón (2010, pág. 74) explica que "La teoría de agentes surge como una evolución de la inteligencia artificial distribuida. La evolución del software, y más concretamente del software que incorpora elementos de la

inteligencia artificial, tiende a la creación de entidades con comportamientos y conductas similares a las de los humanos."

Wooldridge(2002), Mas,(2005) Puntualizan lo siguiente "Un sistema multi-agente se define como cualquier sistema compuesto de múltiples agentes autónomos con capacidades incompletas para resolver un problema global, en donde no existe un sistema de control global, los datos son descentralizados y la computación es asincrona."

Por otra parte el ingeniero José Bañares (2006)"Los agentes software surgen dentro del campo de la Inteligencia Artificial y, a partir de los trabajos desarrollados en el área de la Inteligencia Artificial Distribuida (DAI), surge el concepto de sistemas Multiagente."

Con el transcurrir de los años la mente humana no conoce de límites, mientras la tecnología avanza surge nuevas metodologías para resolver problemas, una de estas son las tecnologías de agentes que incorpora las características como, inteligencia artificial, aprendizaje automático, desenvolvimiento en el medio que se encuentra, dando así soluciones a problemas como en este caso la detección de intrusos.

2.3.2. Razonamiento basado en casos

López De Mantaras y Plaza, (1997).E1 razonamiento basado en casos es un tipo de razonamiento, utilizado en el pensamiento humano, en el que se recurre a experiencias pasadas para resolver nuevos problemas.

Para el Ing. Cristian Pinzón (2010). El CBR (*razonamiento basado en casos*) es otro paradigma de resolución de problemas, pero con diferencias sustanciales con el resto de los acercamientos de la inteligencia artificial, haciéndolo atractivo para abordar diferentes tipos de problemas.

La aplicación de modelos CBR requiere tener en cuenta dos aspectos importantes. En primer lugar, el modelo se basa en la idea de que problemas similares tienen soluciones similares. Sin embargo, carecer de problemas similares no supone que el sistema no sea capaz de proponer buenos resultados, sino que la reutilización de

memorias pasadas se convierte entonces en un proceso creativo. Sea cual sea el resultado de este proceso creativo, el individuo aprende de la nueva experiencia. En segundo lugar, en el proceso de razonamiento explicado se está emitiendo un juicio de valor que permite saber si la solución aplicada para resolver un determinado problema fue buena o no fue buena. Si este juicio es emitido por un experto en la materia del problema resuelto, mayores serán las posibilidades de incrementar la capacidad de aprendizaje (Schank, 1983).

Este tipo de razonamiento se basa en la lógica humana tomando en cuenta experiencias pasadas para dar solución a nuevos problemas proponiendo nuevos y buenos resultados.

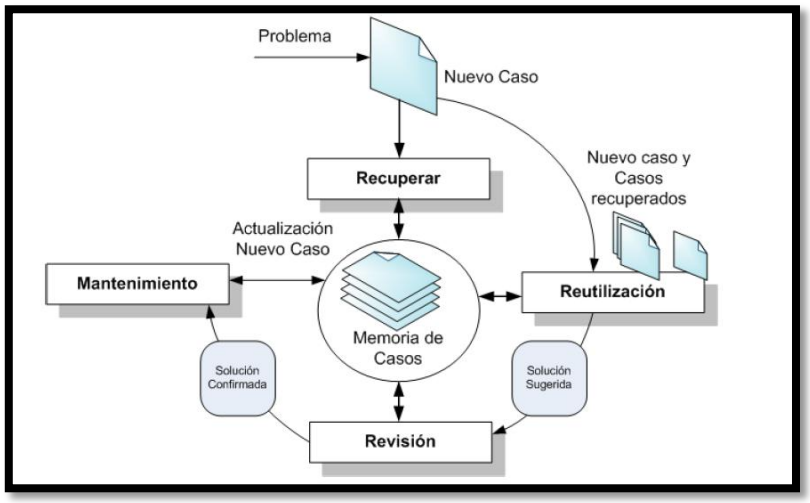


Figura 4: El ciclo del CBR según la UDT-IA

Autores: Aamodt y Plaza, 1994

2.3.3. Aprendizaje automático y minería de datos

La detección de intrusión es una de las tecnologías claves de la seguridad informática centrada en la identificación de actividades maliciosas, siendo la estrategia de detección basada en usos indebidos (firmas de ataque) el enfoque más aplicado. Sin embargo, como ya se ha mencionado anteriormente, su limitación principal está en el

mantenimiento costoso de la base de datos de firmas para mantener la efectividad en la detección. Para superar esta y otras limitaciones, la aplicación de técnicas de minería de datos y aprendizaje automático se le han convertido en la nueva línea de investigación en los IDS

Witten y Frank, (2000), La minería de datos es el proceso de extraer conocimiento útil y comprensible, previamente desconocido, desde grandes cantidades de datos almacenados en distintos formatos .

Alpaydin, (2004), Mientras que el aprendizaje automático se ocupa de desarrollar algoritmos capaces de aprender, y constituye, junto con la estadística, el corazón del análisis inteligente de los datos. El modelo construido puede ser predictivo para hacer predicciones en el futuro, descriptivo para ganar conocimiento de los datos, o sencillamente la aplicación de ambos.

Una característica principal dentro de las técnicas de aprendizaje es el paradigma de aprendizaje de los sistemas. En el aprendizaje supervisado, se realiza la estimación basada en un conjunto de entrenamiento, que incluye la clase a la que pertenecen los ataques. Dicha estimación se extrae mediante la utilización de diversos algoritmos sobre un conjunto de registros de ataques previamente etiquetados.

En cambio, en el aprendizaje no supervisado, el sistema de clasificación de patrones debe diseñarse partiendo de un conjunto de patrones de entrenamiento para los cuales no conocemos sus etiquetas de clase. Estas situaciones se presentan cuando no disponemos del conocimiento de un experto o bien cuando el etiquetado de cada muestra individual es impracticable.

Tsai, etal., (2009). En el campo de la detección de intrusión, se ha venido realizando un gran número investigaciones utilizando numerosas técnicas de aprendizaje. Aquí, la minería de datos y los métodos de aprendizaje automático se centran en el análisis de las propiedades de los patrones de auditoría en lugar de identificar el proceso que los genera.

La minería de datos tiene como objetivo clave extraer conocimientos útiles y comprensibles dentro de una cantidad de información para desarrollas algoritmos de técnicas aprendizaje.

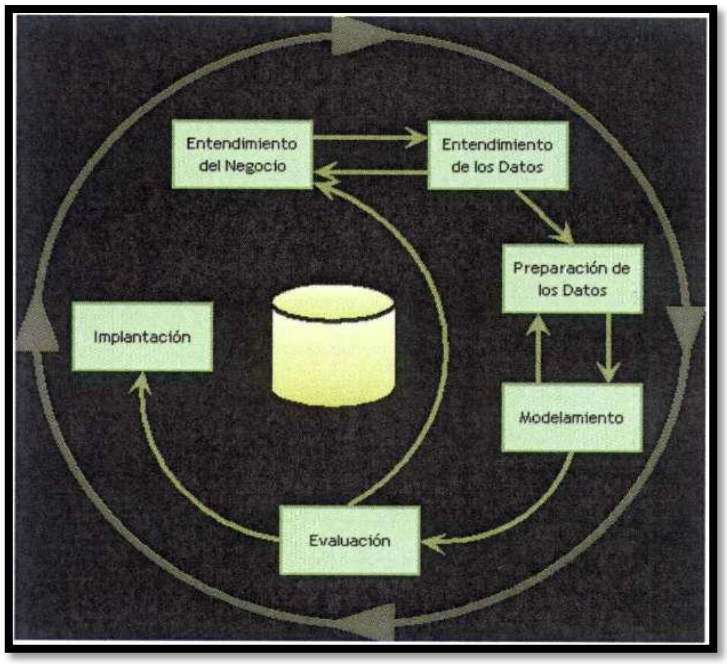


Figura 5 : Pasos del proceso de minería de datos

Autor: William Pullutaxi

2.3.4. Sistemas multiagente

2.3.4.1.Concepto de agente

Wooldridge, (2002) define un agente como un sistema computacional que se sitúa en algún entorno y es capaz de actuar de forma autónoma en dicho entorno para alcanzar sus objetivos de diseño. Otra definición de agente desde otra perspectiva es dada por (Russel y Norvig, 1995), quien considera que un agente es cualquier cosa capaz de percibir su entorno a través de sensores y responder según su función en el mismo entorno a través de actuadores, asumiendo que cada agente puede percibir sus

p-opias acciones y aprender de la experiencia para definir su comportamiento. En la Figura 6 se muestra una representación de la anatomía de un agente

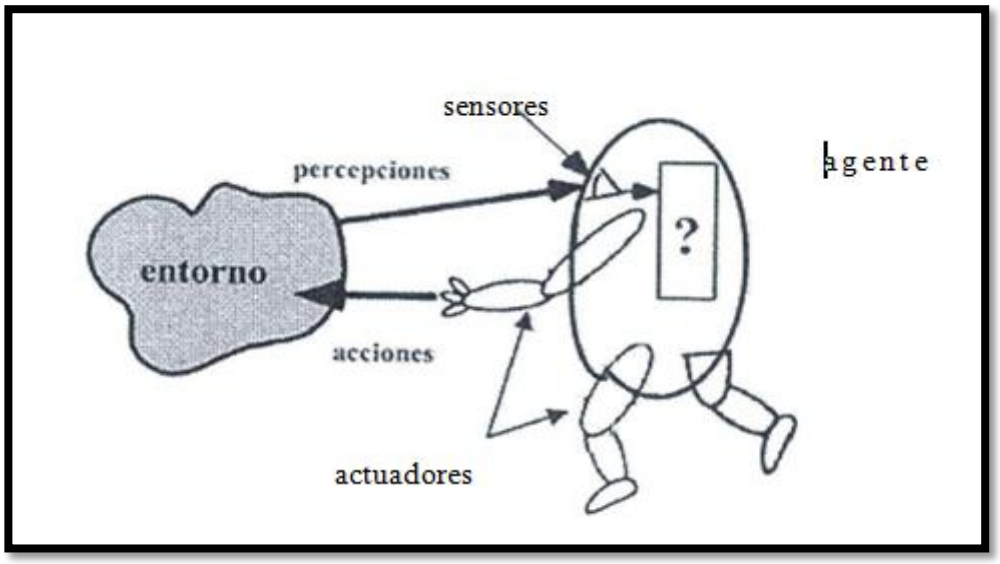


Figura 6: Anatomía de un agente

Autor: Jones, 2008

Adicional a esta característica, hay que añadir otras que los agentes deben cumplir:

Inteligencia: Rodearse de conocimiento (creencias, deseos, intenciones y metas).

- Aprendizaje. Habilidad de adaptarse progresivamente a cambios en entornos dinámicos, mediante técnicas de aprendizaje.
- Reactividad. Percibir su entorno y actuar sobre éste con la capacidad de adaptarse a sus necesidades.
- Pro-Actividad o Racionalidad. Tomar la iniciativa para definir metas y planes que les permitan alcanzar sus objetivos.
- Movilidad: Capacidad para moverse de un sitio a otro.
- Situación. Situarse dentro de un entorno, ya sea real o virtual.
- Habilidad social. Interactuar con otros agentes, incluso con humanos.

2.3.4.2.Concepto de Sistemas Multi-Agente

Mas, (2005).Una vez descritos los principales requisitos que debe cumplir un agente y las características de los diferentes tipos de agentes que existen, es necesario definir lo que es un sistema multi-agente (MAS, Multi-AgentSystem). Se considera un sistema multi-agente cuando dos o más agentes son capaces de trabajar de forma conjunta con el objetivo de resolver un problema

Wooldridge, (2002): Un sistema basado en agentes, puede contener uno o más agentes (Corchado y Molina, 2002), pero solo utiliza el concepto de agente como mecanismo de abstracción, ya que a la hora de implementarlo no existe alguna estructura de software correspondiente a éstos. Contrario a un sistema multi-agente que debe cumplir una serie de condiciones

Al menos uno de los agentes debe de ser autónomo y debe existir al menos una relación entre dos agentes en la que se cumpla que uno de los agentes satisface el objetivos del otro. Esto quiere decir que al menos uno de los agentes dispone de información incompleta o de capacidades limitadas para resolver el problema.

- Los sistemas multi-agente se caracterizan porque no existe un sistema control global y porque cada agente se centra en su conducta individual.
- Por otro lado, los datos se encuentran organizados de forma distribuida (descentralizados), lo que favorece su computación asíncrona.
- Cada agente puede decidir con libertad, dinámicamente, que tareas debe efectuar y a quien asigna estas tareas

Finalmente, los sistemas multi-agente han evolucionado durante los últimos años, tratando de adaptarse a los cambios que presentan las nuevas tecnologías. El papel que juega el entorno es cada vez más importante en los sistemas multi-agente.

Hoy en día las personas disponen de dispositivos móviles, con lo que es frecuente que un agente que se ejecuta en un dispositivo móvil cambie frecuentemente de un entorno a otro. Además, cada vez es más frecuente encontrar dispositivos inteligentes que pueden interactuar con los agentes de forma automática.

Así pues, los sistemas multi-agente necesitan modelar el entorno en el que se encuentran y desarrollar mecanismos de comunicación adecuados con los elementos de dicho entorno. Esto supone la necesidad de ampliar los conceptos utilizados en las metodologías de desarrollo así como desarrollar nuevos mecanismos de comunicación y nuevas herramientas de implantación.

2.3.5. Seguridad Informática

Un sistema informático es seguro si su comportamiento es acorde con las especificaciones previstas para su utilización.

Seguridad es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables.

Riesgos que puede sufrir la información.

- Revelación : Acceso no autorizado a información Engaño : Admisión de datos falsos
- Perturbación : Interrupción o prevención de correcta operación
- Usurpación: Control no autorizado de partes del sistema Fisgoneo:
- Captura no autorizada de información (forma pasiva de revelación).
- Solución : Servicio de confidencialidad
- Modificación: cambio no autorizado de información (engaño, perturbación, usurpación).
- Solución : servicio de integridad
- Enmascaramiento: una entidad hace pasarse por otra (engaño, usurpación).
- Solución : servicio de integridad
- Una forma permitida de enmascaramiento: Delegación de Autoridad.

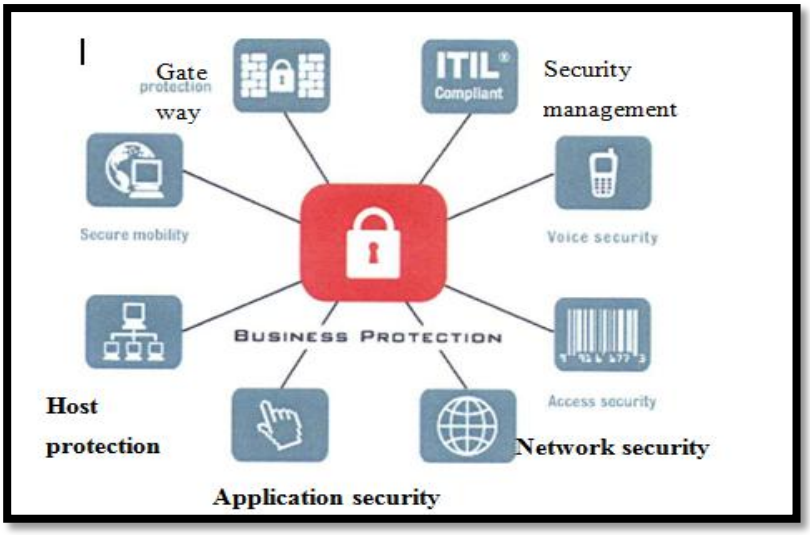


Figura 7: Protecciones de la información

Autor: William Pullutaxi

Tipos de seguridad

Básicos:

- Confidencialidad (Privacidad): Mecanismos de control de accesos: Criptografía.
- Ley de protección de datos.
- Integridad: de datos o de origen (autentificación)
- Mecanismo de prevención : gestión modificaciones autorizadas
- Mecanismos de detección
- Disponibilidad
- Ataques de denegación de servicio
- Adicionales: Consistencia, Control, Auditoría.

La seguridad informática se refiere a mantener la integridad disponibilidad y confidencialidad de datos, es decir mantener la información segura ante los ciber delincuentes que día a día aparecen, los mismos que pueden robar la información con fines maliciosos, haciendo uso de ellos para su conveniencia.

2.3.6. Delitos informáticos

El ser humano poco a poco, logró automatizar muchas de sus actividades. Se ahorra tiempo y recursos con el empleo de lo que se denomina "inteligencia artificial". Es difícil imaginar alguna actividad humana en la que no intervengan máquinas dotadas de gran poder de resolución.

La informática, entendiéndola como el uso de computadoras y sistemas que ayudan a mejorar las condiciones de vida del hombre, la encontramos en todos los campos: en la medicina, en las finanzas, en el Derecho, en la industria, entre otras. En la actualidad con la creación de la denominada "autopista de la información", el INTERNET, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento. El problema radica en que, la conducta humana parece ser que está inclinada al delito, a conseguir satisfacción a sus deseos a toda costa. Con el desarrollo de la informática, aparece también lo que se denomina como: DELITO INFORMATICO.

De la misma manera que muchas personas se han dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras tratan de utilizar la tecnología, y en el caso que nos ocupa, las computadoras y sistemas, para el cumplimiento de actividades ilícitas.

De la misma forma como se encuentran cosas positivas en el INTERNET, encontramos cosas negativas, lo cual nos lleva a pensar que el mal no está en la tecnología sino en las personas que las usan, a modo de ejemplificación diremos que la red de comunicación electrónica digital, se la ha utilizado por pederastas para estimular la prostitución infantil, del mismo modo grupos políticos racistas neo nazis lo han usado para difundir su nefasta ideología, se cree, inclusive, que el INTERNET es una vía de comunicación y negocios entre narcotraficantes y contrabandistas de armas, etc.

Tipos de Delitos Informáticos

Las Naciones Unidas reconocen como delitos informáticos los siguientes:
Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de datos de entrada
- Manipulación de programas.
- Manipulación de los datos de salida.

Falsificaciones informáticas:

- Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Cuando se usan las computadoras para efectuar falsificaciones de documentos de uso comercial.
- Daños o modificaciones de programas o datos computarizados: Sabotaje informático mediante: virus, gusanos, bomba lógica o cronológica.
- Acceso no autorizado a servicios y sistemas informáticos. Piratas informáticos o hackers.
- Reproducción no autorizada de programas informáticos de protección legal.

2.3.7. Sistemas de detección de intrusos

Los Sistemas de Detección de Intrusión, de ahora en adelante simplemente IDS, son sistemas que monitorizan el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información Wu y Banzhaf, (2010).

Una intrusión se puede definir como toda actividad no autorizada que no debería ocurrir en el sistema. Una intrusión materializada (ataque) viola las políticas de

seguridad de un sistema y compromete la integridad, confidencialidad y disponibilidad de los recursos. Los IDS generalmente deben cumplir algunas características deseables independientemente de qué sistema vigile o su forma de trabajar, que incluyen:

- Una ejecución continúa de forma transparente, y con un mínimo de supervisión.
- Capacidad de tolerancia a fallos. Capacidad para recuperarse de posibles fallos o problemas con la red.
- Capacidad para identificar si alguno de sus componentes ha sido comprometido, e intentar recuperar dicho componente, y en caso contrario administrar un tipo de alerta.
- Minimizar el consumo de recursos.
- El Sistema de Detección de Intrusos debe permitir aplicar una configuración según las políticas de seguridad que dicte la organización.
- Capacidad de adaptación. La capacidad de adaptarse a los rápidos cambios que sufren los sistemas y los usuarios. Además de incluir un proceso rápido y sencillo de actualización.

2.3.8. Ataques en entornos dinámicos y distribuidos

La seguridad de la información se basa en tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad, más conocidos como "The Big Three" (C.I.A) (Krutz y Vines, 2002). En función de la aplicación y el contexto, cada principio puede jugar un papel más importante que el resto. No obstante, debe quedar claro que todos los controles y las medidas de seguridad, todas las amenazas y vulnerabilidades, y los procesos de seguridad son medidos desde el punto de vista de estos tres principios

- **Confidencialidad**

La confidencialidad es el hecho de prevenir la divulgación de información a personas o sistemas no autorizados.

Un claro ejemplo de confidencialidad es la de una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

- **Integridad**

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información

- **Disponibilidad**

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de

comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Los ataques en entornos dinámicos y distribuidos hoy en día crece a pasos agigantados poniendo en evidencia la falta de políticas de seguridad que tiene una Institución, poniendo en riesgo información confidencial que al ser extraída puede ser utilizada para perjudicar a la misma.

2.4.Hipótesis

La aplicación de un Sistema Multi-Agente influirá en la detección de ataques en entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY

Unidades de Observación: Empresa Importadora REPCOPY

2.5.Señalamientos de Variables

Variable Independiente

Sistemas Multiagente

Variable dependiente

Ataques en entornos dinámicos y distribuidos

CAPÍTULO III

MARCO METODOLÓGICO

3.1.Enfoque

El presente trabajo investigativo tomará un enfoque cuali-cuantitativo por las siguientes consideraciones:

Cualitativa porque se considera mucho la participación de las personas que se encuentran dentro de la Institución con sus diferentes opiniones y sugerencias, también se enmarcará en el aspecto interpretativo ya que los resultados obtenidos servirán para la toma de decisiones.

Cuantitativo porque la solución al presente problema tendrá una normativa que guiará el desarrollo de la investigación.

3.2.Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad bibliográfica o documentada: Se ha considerado esta modalidad ya que se ha obtenido la información de libros, libros virtuales, tesis de grados, repositorios de tesis.

Modalidad experimental: Se ha considerado la relación de la variable independiente "Sistemas Multi-Agente" y su influencia y relación en la variable dependiente detección de ataques en entornos dinámicos y distribuidos para considerar sus causas y sus efectos.

Modalidad de campo: Se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente de los involucrados a través de una encuesta.

3.3.Tipos de investigación

Se ha realizado la investigación exploratoria ya que permitió plantear el problema de investigación Estudio de los Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY, de la misma manera ayudo a plantear la hipótesis la aplicación de un Sistema Multi-Agente permite la detección de ataques en entornos dinámicos y distribuidos de la Institución.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente "Sistemas Multi-Agente" con la variable dependiente detección de ataques en entornos dinámicos y distribuidos para considerar sus causas y sus efectos.

3.4.Población y Muestra

La población considerada para la siguiente investigación son: 10 empleados que laboran en la Institución.

3.5.Operacionalización de variables

Hipótesis: La aplicación de un Sistema Multi-Agente influirá en la detección de ataques en entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY

Variable independiente: Sistemas Multi-Agente ***Continua en la página 30***

CONCEPTO	CATEGORÍAS	INDICADORES	ÍTEMS	TÉCNICAS / INSTRUMENTOS
Es un <u>sistema informático</u> capaz de tener <u>acción independiente</u>	Sistema Informático	Software Recurso Humano	¿Ha tenido en cuenta la posibilidad de perder la información, que no se correcta o que se roben? ¿Se hace algún tipo de revisión del sistema de información de forma periódica? ¿Se ha definido niveles de acceso a los usuarios, es decir a que tienen acceso y a que no? ¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios	Encuesta a través de un cuestionario aplicado a los usuarios de la Empresa

	Acción Independiente	Minería de datos Inteligencia artificial	no autorizados? ¿Existe un responsable o responsables que coordinen las medidas de seguridad? ¿Dispone la Empresa de herramientas o sistemas que detecten los intentos de acceso a la red de la Empresa?	

Tabla 1: Operacionalización de variable Independiente

Autor: William Pullutaxi

Variable dependiente: detección de ataques en entornos dinámicos y distribuidos ***Continua en la página 32***

CONCEPTO	CATEGORÍAS	INDICADORES	ÍTEMS	TÉCNICAS / INSTRUMENTOS
Sistema que detecta hackers malintencionados no deseadas en el sistema, especialmente a través de Internet.	Hackers Internet	Conocimiento Acción maliciosa Datos Información red	¿Existen controles que detecten posibles fallos en la seguridad? ¿Cuenta la Empresa con una política de seguridad? ¿Se realizan copias de seguridad de la información, con qué frecuencia? ¿Se ha elaborado un plan de seguridad en la Empresa? ¿Tiene la Empresa elaborado un plan de contingencia?	Encuesta a través de un cuestionario aplicado a los usuarios de la Empresa

			¿Existe un presupuesto asignado para la seguridad en la Empresa? ¿Existe una política definida para los accesos a Internet? ¿Existen controles sobre las páginas accedidas por cada usuario? ¿Se revisan las páginas accedidas para tomar medidas contra los usuarios que no cumplan sus funciones?	

Tabla 2: Operacionalización de variable Dependiente

Autor: William Pullutaxi

3.6.Recolección y análisis de la información

SECUNDARIA	PRIMARIA
• **Se recolecta de estudios realizados anteriores que se encuentran en las tesis.**	Se recolecta directamente del contacto con los usuarios de las bases de datos y redes de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.
• **Se encuentran registrada en libros, tesis de grado, archivos de la Web**	
• **Las fuentes de información son: biblioteca de la Facultad, Internet, repositorios de tesis**	

Tabla 3: Recolección y análisis de la información.

Autor: William Pullutaxi

Técnicas de Investigación

BIBLIOGRÁFICAS	DE CAMPO
• El análisis de documentos (lectura científica).	• La entrevista
• El fichaje	• La encuesta

Tabla 4: Técnicas de Investigación

Autor: William Pullutaxi

Recolección de la información Autor:

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	A los empleados de la Empresa Importadora REPCOPY
3. ¿Sobre qué aspectos?	**V.I:** Sistemas Multi-Agente **V.D:** Ataques en entornos dinámicos y distribuidos

4. ¿Quién?	Investigador
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿lugar de recolección de la información?	Empresa Importadora REPCOPY
7. ¿Cuántas veces?	1 sola vez.
8. ¿Qué técnicas de recolección?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

Tabla 5: Recolección de la Información

Autor: William Pullutaxi

3.7.Procesamiento y análisis de la información

- Revisión y codificación de la información
- Categorización y tabulación de la información
- Tabulación Manual
- Tabulación computarizada: programa SPSS
- Análisis de los datos.
    - La presentación de los datos se lo hará en gráficos cuadros para analizarlos e interpretarlos
- Interpretación de los resultados
- Describir los resultados
- Analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.
- Estudiar cada uno de los resultados por separado
- Redactar una síntesis general de los resultados.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE DATOS

La siguiente encuesta se realizó a las 10 personas que laboran dentro de la Empresa Importadora REPCOPY obteniendo los resultados que se muestran a continuación.

4.1. Análisis de resultados

1. **¿Ha tenido en cuenta la posibilidad de perder la información, que no sea correcta o que se roben?**

N	ITEMS	FRECUENCIA	%
1	Si	10	100%
2	No	0	0%
3	en blanco	0	0%
Total		10	100%

Tabla 6: Frecuencia de la Pregunta N°1

Autor: William Pullutaxi

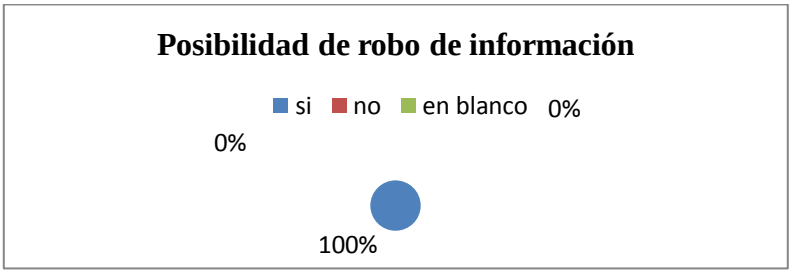


Figura 8: Posibilidad de robo de información

Análisis:

El 100% de los encuestados que representa a todo el personal que labora en la Empresa nos indica que, tiene en cuenta sobre el peligro de trabajar vía una red de datos, los problemas que pueden tener y las amenazas de las que pueden ser víctimas.

2. ¿Cuenta la Empresa con una política de seguridad?

N	ITEMS	FRECUENCIA	%
1	si	0	0%
2	no	8	80%
3	en blanco	2	20%
Total		10	100%

Tabla 7: Frecuencia de la pregunta N°2

Autor: William Pullutaxi

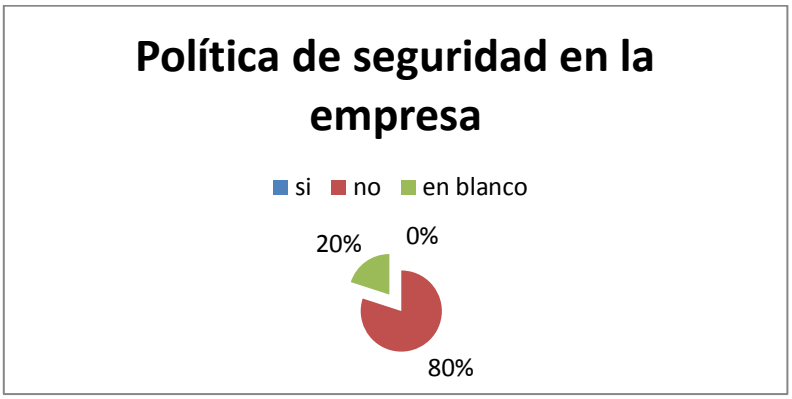


Figura 9: Política de seguridad

Autor: William Pullutaxi

Análisis:

El 80% que representa a 8 personas nos indica que la Empresa no cuenta con una política de seguridad, mientras que el 20% que representa a 2 personas tienen el desconocimiento de si hay o no hay una política.

3. **¿Existen controles que detecten posibles fallos en la seguridad?**

N	ITEMS	FRECUENCIA	%
1	si	0	0%
2	no	7	70%
3	en blanco	3	30%
Total		10	100%

Tabla 8: Frecuencia de la pregunta N°3

Autor: William Pullutaxi

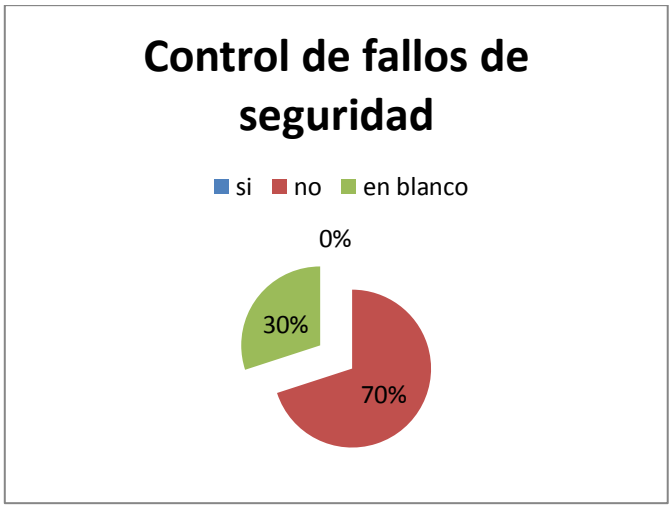


Figura 10: Control de fallos de seguridad

Autor: William Pullutaxi

Análisis:

De las 10 personas encuestadas no hay una sola persona que indica que en las redes de la Empresa Importadora REPCOPY existen controles en fallos de la seguridad, el 70% que representa 7 personas manifestaron que no existen control en el fallo de seguridad, y el 30% que representa 3 personas no saben si existen control alguno de los fallos de la seguridad

4. **¿Se hace algún tipo de revisión del sistema de información de forma periódica?**

N	ITEMS	FRECUENCIA	%
1	Si	1	10%
2	No	8	80%
3	en blanco	1	10%
Total		10	100%

Tabla 9: Frecuencia de la pregunta N°4

Autor: William Pullutaxi

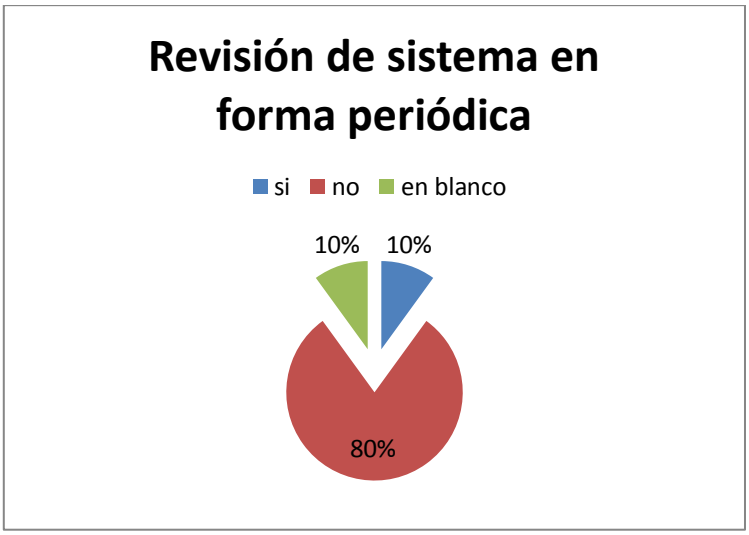


Figura 11: Revisión de sistema en forma periódica

Autor: William Pullutaxi

Análisis:

De las 10 personas encuestadas el 10% que representa 1 personas indican que el sistema de información que maneja la Empresa es revisada de forma periódica, el 80% que representa 8 personas manifestaron que no se da la revisión del sistema periódicamente y está presenta fallas constantemente.

5. **¿Se ha definido niveles de acceso a los usuarios, es decir a que tienen acceso y a que no?**

N	ITEMS	FRECUENCIA	%
1	Si	9	90%
2	No	0	0%
3	en blanco	1	10%
Total		10	100%

Tabla 10: Frecuencia de la pregunta N°5

Autor: William Pullutaxi

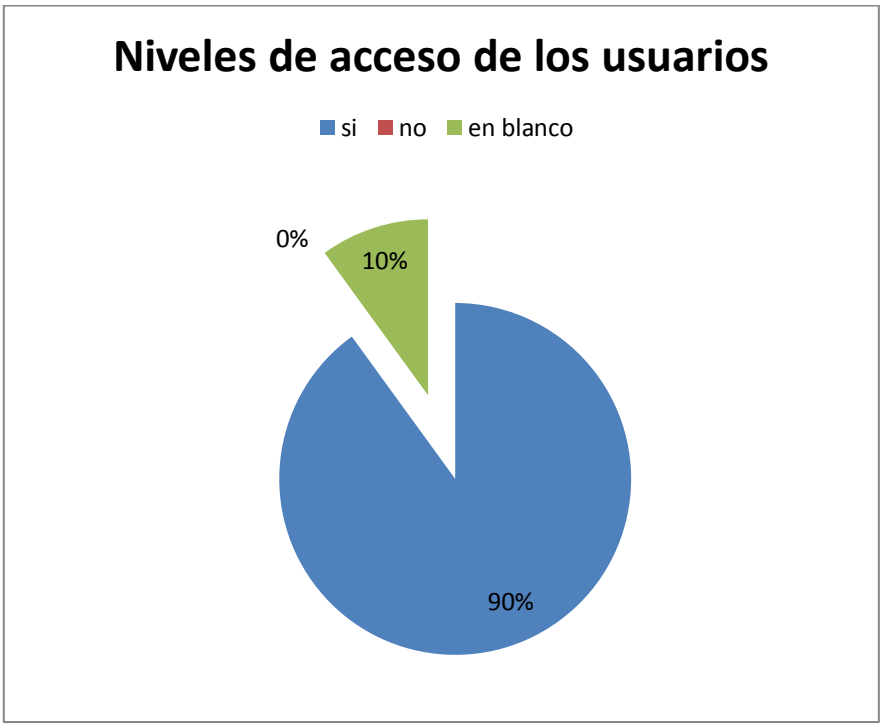


Figura 12: Niveles de acceso de los usuarios

Autor: William Pullutaxi

Análisis:

El 90% de las personas encuestadas que representa 9 personas indican que en la Empresa, para el manejo del sistema informático tienen asignado niveles de acceso para los usuarios, dando acceso solo a la información que ellos deben manejar.

6. **¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?**

N	ITEMS	FRECUENCIA	%
1	si	1	10%
2	no	5	50%
3	en blanco	4	40%
Total		10	100%

Tabla 11: Frecuencia de la pregunta N°6

Autor: William Pullutaxi

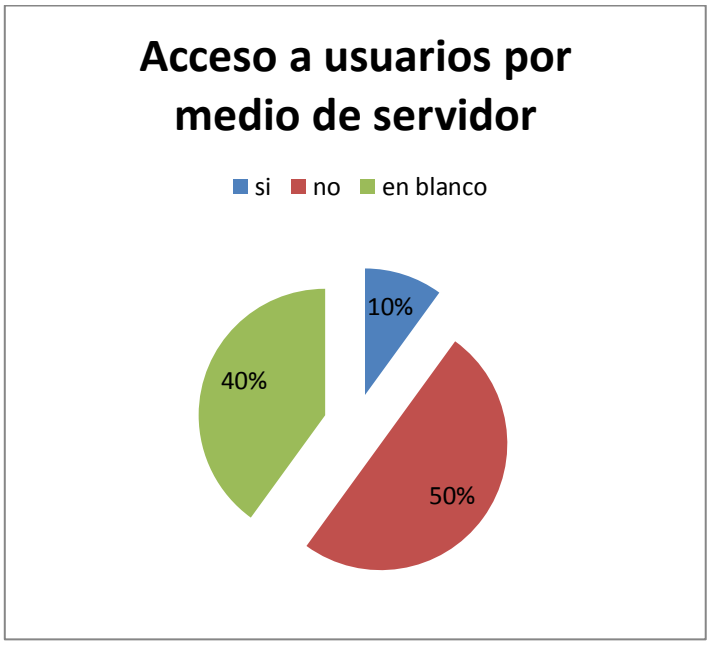


Figura 13: Acceso a usuarios por medio del servidor

Autor: William Pullutaxi

Análisis:

El 50% que representa 5 personas indican que no existe servidores que impiden el acceso a los usuarios no autorizado a la base de datos de la Empresa, mientras que el 40% que representa a 4 personas no contestaron a esta pregunta, y el 1% que representa a una persona indica que el servidor de la Empresa si restringe el acceso a los usuarios no autorizados.

7. **¿Se realizan copias de seguridad de la información, con qué frecuencia?**

N	ÍTEMS	FRECUENCIA	%
1	cada día	9	90%
2	cada semana	0	0%
3	cada mes	0	0%
4	nunca	0	0%
5	en blanco	1	10%
Total		10	100%

Tabla 12: Frecuencia de la pregunta N°7

Autor: William Pullutaxi

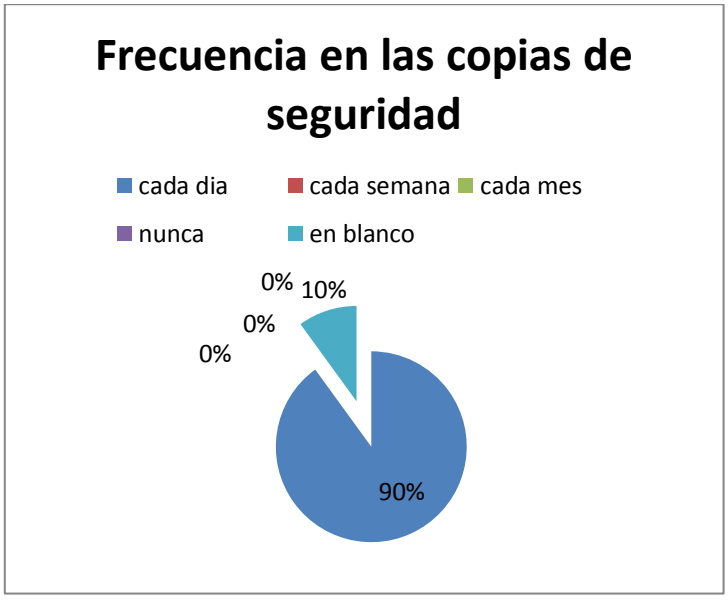


Figura 14: Frecuencia en las copias de seguridad

Autor: William Pullutaxi

Análisis:

El 90% de las personas representadas por 9 personas indican que se realiza una copia de las bases de datos diariamente manteniendo así un respaldo de seguridad, mientras que el 10% que representa 1 persona indica no saber si realizan copias de seguridad o no.

8. ¿Se ha elaborado un plan de seguridad en la Empresa?

N	ITEMS	FRECUENCIA	%
1	SI	0	0%
2	No	7	70%
3	En Blanco	3	30%
Total		10	100%

Tabla 13: Frecuencia de la pregunta N°8

Autor: William Pullutaxi

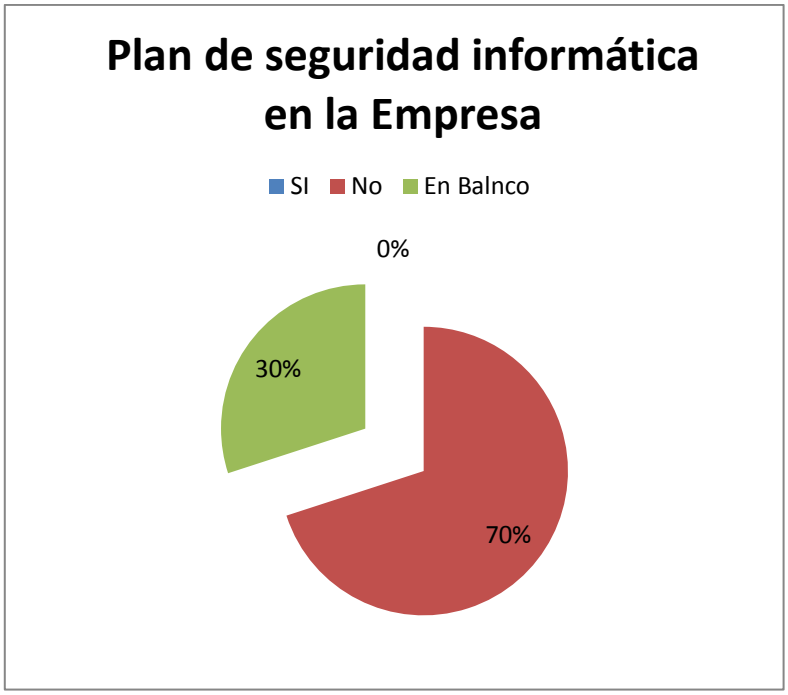


Figura 15: Plan de seguridad

Autor: William Pullutaxi

Análisis

El 70% de las personas indican que la Empresa no cuenta con un plan de seguridad informática, mientras que el 30% no contestan a esta pregunta dando a entender que no saben si hay o no hay un plan de seguridad informática.

9. **¿Existe un responsable o responsables que coordinen las medidas de seguridad?**

N	ITEMS	FRECUENCIA	%
1	SI	0	0%
2	No	8	80%
3	En Blanco	2	20%
Total		10	100%

Tabla 14: Frecuencia de la pregunta N°9

Autor: William Pullutaxi

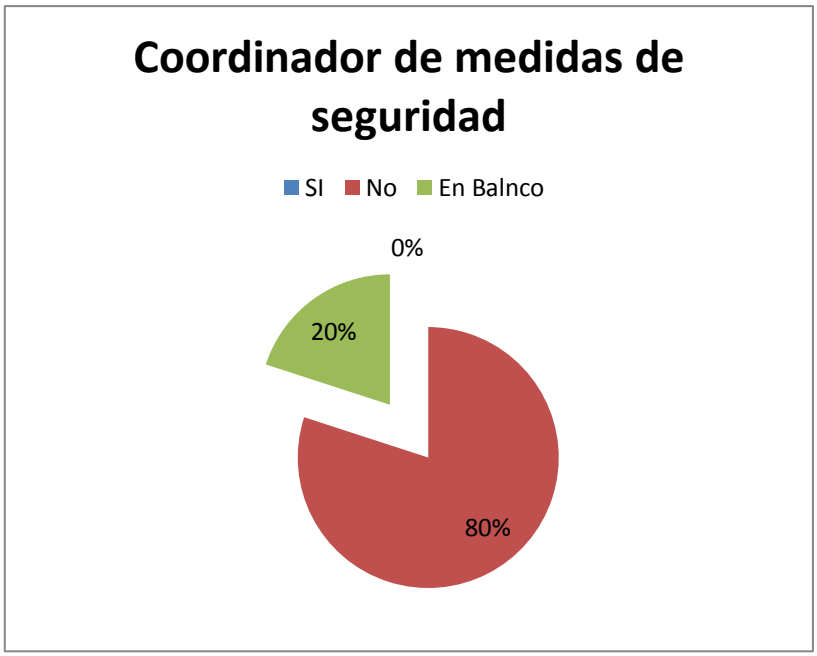


Figura 16: Coordinador de medidas de seguridad

Autor: William Pullutaxi

Análisis

La 80% de las personas indicaron que no existe un responsable en la Empresa que coordine la seguridad de la misma, mientras que el 20% desconocen de esta situación.

10. ¿Tiene la Empresa elaborado un plan de contingencia?

N	ITEMS	FRECUENCIA	%
1	SI	0	0%
2	No	6	60%
3	En Blanco	4	40%
Total		10	100%

Tabla 15: Frecuencia de la pregunta N°10

Autor: William Pullutaxi

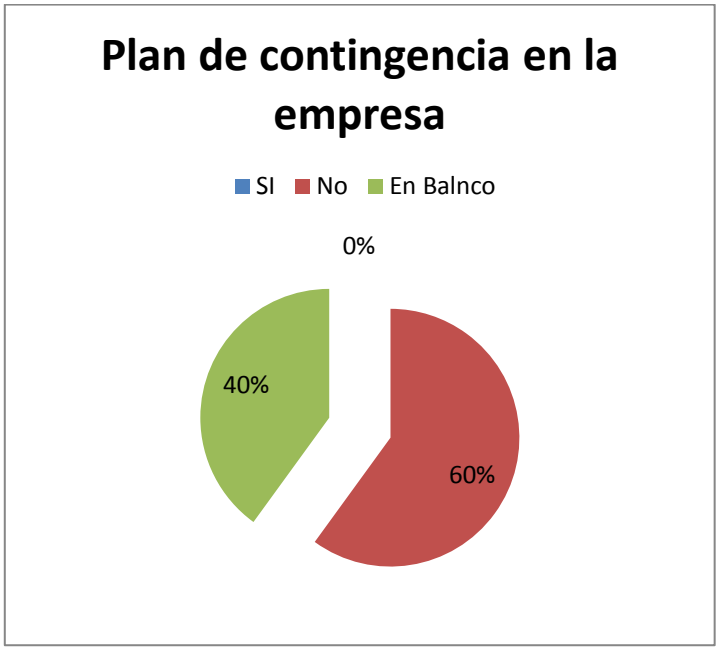


Figura 17: Plan de contingencia en la Empresa

Autor: William Pullutaxi

Análisis

El 40% de los encuestados no tienen conocimientos de que la Empresa cuente con un plan de contingencia ante cualquier ataque en la red institucional, mientras que el 60% de los encuestados indican que la Empresa no tiene un plan de contingencia vigente.

11. ¿Existe un presupuesto asignado para la seguridad en la Empresa?

N	ITEMS	FRECUENCIA	%
1	SI	0	0%
2	No	7	70%
3	En Blanco	3	30%
Total		10	100%

Tabla 16: Frecuencia de la pregunta N°11

Autor: William Pullutaxi

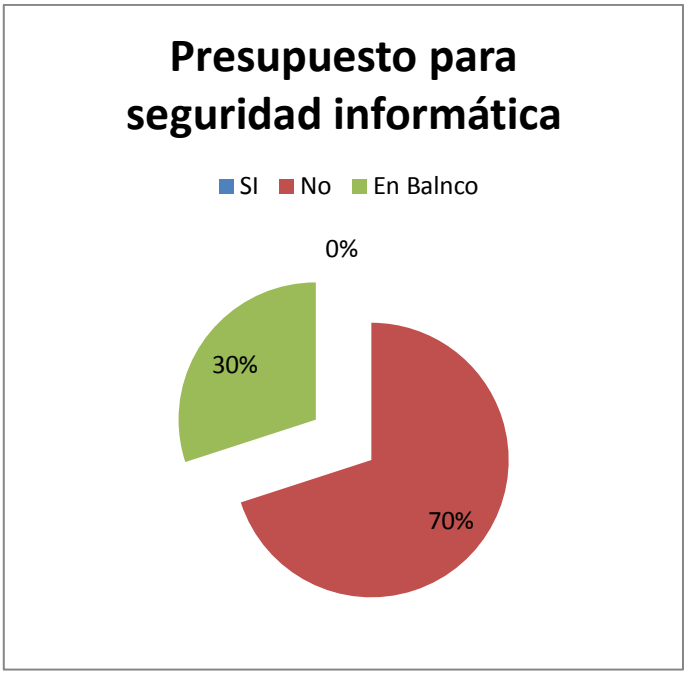


Figura 18. Presupuesto para seguridad informática

Autor: William Pullutaxi

Análisis

La Empresa no le toma mucha importancia a la seguridad de la información es por ello que el 30% indican no conocer acerca de los presupuestos de la Empresa, mientras que el 70% indican que no asignan un presupuesto para precautelar la información.

12. ¿Existe una política definida para los accesos a Internet?

N	ITEMS	FRECUENCIA	%
1	SI	1	10%
2	No	6	60%
3	En Blanco	3	30%
Total		10	100%

Tabla 17: Frecuencia de la pregunta N°12

Autor: William Pullutaxi

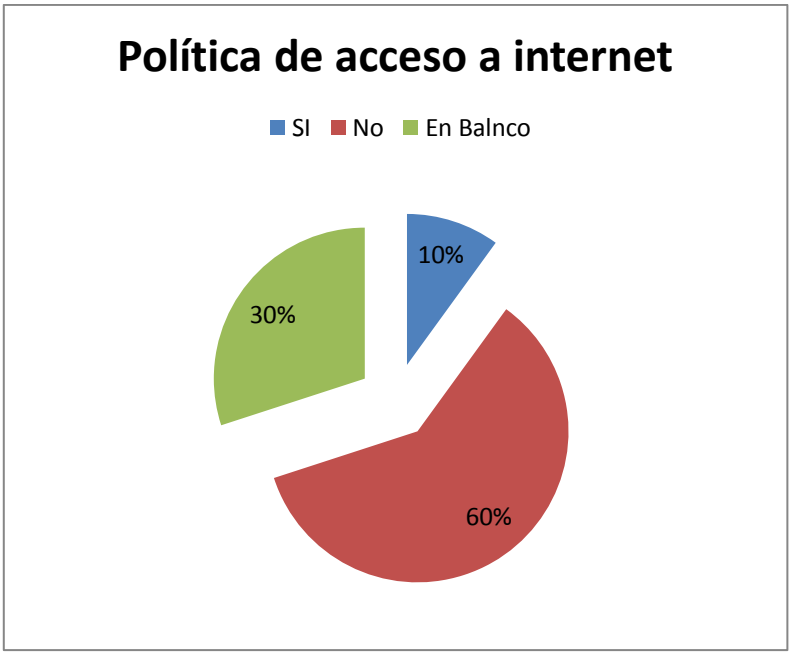


Figura 18: Política de acceso a Internet

Autor: William Pullutaxi

Análisis

El 10% de los encuestados indican que si hay políticas de seguridad en cuanto acceso a Internet se refiere, mientras que el 30% indican no saber, y el 60% indican que no hay control alguno sobre el acceso al Internet.

13. ¿La Empresa ha sufrido algún ataque ya sea por virus, terceras personas u otro tipo de amenaza?

N	ITEMS	FRECUENCIA	%
1	SI	6	60%
2	No	1	10%
3	En Blanco	3	30%
Total		10	100%

Tabla 18: Frecuencia de la pregunta N°13

Autor: William Pullutaxi

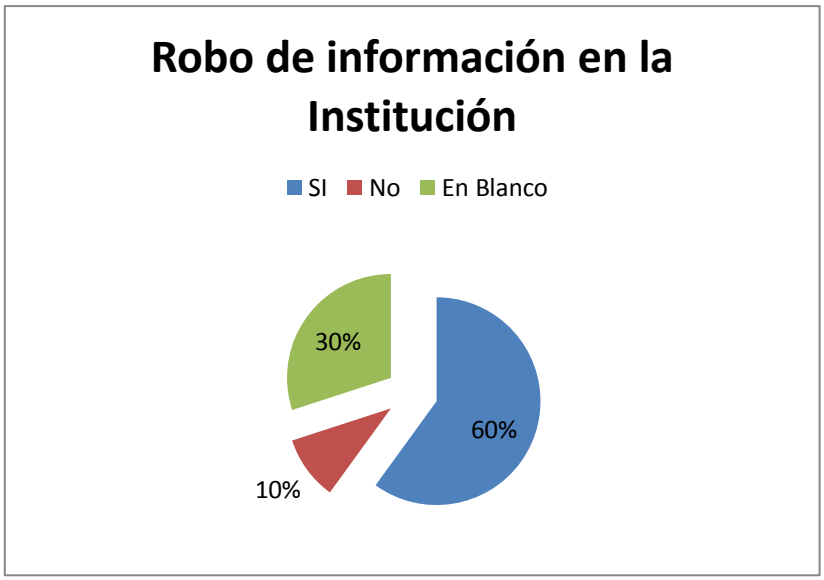


Figura 19: Robo de información en la Empresa

Autor: William Pullutaxi

Análisis

En la Empresa el 30% de las personas encuestadas desconocen sobre el robo de información en la Institución, por otro lado el 10% indican que la Empresa no ha sufrido robo alguno, mientras que la mayoría, es decir el 60% indican que la Empresa ha sido víctima de ataques por virus y terceras personas.

14. ¿Dispone la Empresa de herramientas o sistemas que detecten los intentos de acceso a la red de la Empresa?

N	ITEMS	FRECUENCIA	%
1	SI	1	10%
2	No	6	60%
3	En Blanco	3	30%
Total		10	100%

Tabla 19: Frecuencia de la pregunta N°14

Autor: William Pullutaxi

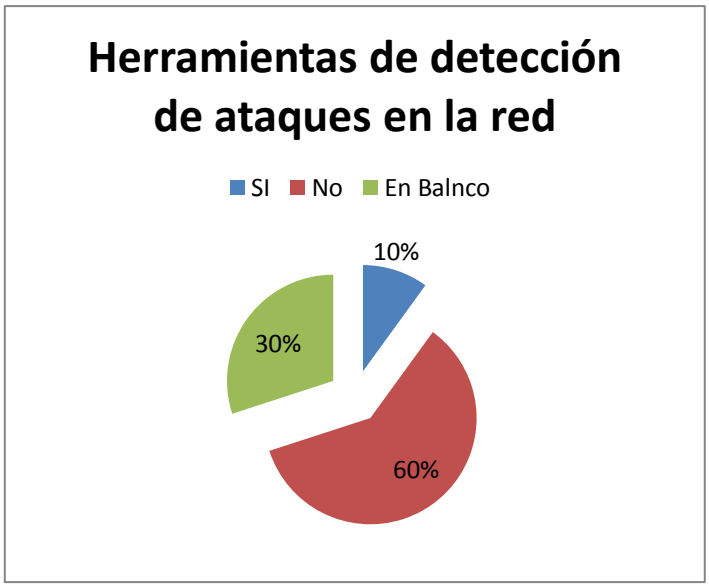


Figura 20: Herramientas de detección de ataques en la red

Autor: William Pullutaxi

Análisis

El 10% de los encuestados que representa a 1 persona indica que en la Empresa existe herramienta para detectar ataques en las redes de la Empresa, mientras que el 60% que representa a 6 personas indican que no existe una herramienta que permita la detección de ataques en los sistemas de la Institución, mientras que el 30% que es 3 personas indican no saber sobre herramienta alguna aplicada en la Empresa.

4.2. Comprobación de la hipótesis

Se ha tomado en cuenta las tres preguntas discriminantes, la numero 9, la numero 13 y la numero 14 de la encuesta aplicada de la Empresa REPCOPY, con los siguientes resultados arrojados.

Pregunta #1. (Pregunta 9)¿Existe un responsable o responsables que coordinen las medidas de seguridad?

Resumen: La Empresa Importadora REPCOPY no cuenta con un encargado de sistemas que pueda dar servicios de seguridad, tanto de los sistemas que manejan así como a la red y algo principal que es el servidor.

Pregunta #2. (Pregunta 13) ¿La Empresa ha sufrido algún ataque ya sea por virus, terceras personas u otro tipo de amenaza?

Resumen: El sistema informático que posee Importadora REPCOPY ha sido atacado por terceras personas lo que ha provocado la mala manipulación de la información y de sus datos perjudicando, tanto en pérdida de tiempo como en pérdidas económicas a la Institución.

Según Leonardo; TENZER, Simón, nos dice que los ataques siempre van a existir y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la Institución.

Pregunta #3. (Pregunta 14) ¿Dispone la Empresa de herramientas o sistemas que detecten los intentos de acceso a la red de la Empresa?

Resumen: La Empresa no cuenta con una herramienta que permita disminuir la vulnerabilidad de su red, provocando así el libre ingreso a los delincuentes informáticos, los que ocasionan pérdida tanto de tiempo como económica.

Interpretación: según las contestaciones del personal de la Empresa los sistemas de información son vulnerables, puesto que no cuentan con una persona capacitada de sistemas que ayude a controlar el buen funcionamiento de la red empresarial, así como también el control sobre la seguridad que deben tener las mismas, es por eso se desea buscar una solución para evitar la pérdida de información y la funcionalidad de la Institución sea eficaz en la prestación de sus servicios.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La Empresa no cuenta con una persona capacitada en el área de Sistemas que ayude a sobrellevar los problemas que esta tiene, es por esto que no se aplican las seguridades necesarias haciendo de estos entornos vulnerables ante cualquier ataque.
- Al no contar la Empresa con una política de seguridad, el personal tiene acceso a cualquier información, estos pueden hacer mal uso de las mismas y causar algún daño institucional.
- Actualmente la Empresa no lleva un control sobre las páginas accedidas por los usuarios, es por esto que el personal tiene acceso a todas las páginas de Internet, impidiendo que el personal cumpla con su responsabilidad en su totalidad.
- La copia de seguridad de la base de datos de la Empresa lo realizan un encargado de forma manual y diariamente, acción que no es muy segura pudiendo esta persona olvidarse de sacar una copia de seguridad, ocasionando que no haya material de respaldo al momento que la Empresa lo requiera causando perdida de información, tiempo y dinero.

- Al no contar la Empresa con una herramienta de seguridad informática hace que esta sea muy vulnerable ante cualquier ataque, provocando robo de información.

5.2. Recomendaciones

- La Empresa debe disponer de personal de sistemas capacitado en el campo de la seguridad tanto de información como de redes, así como también sobre las herramientas avanzadas que día a día aparecen para la detección de ataques, para minimizar las vulnerabilidades de las redes de comunicación.
- Establecer una política de seguridad para los accesos del personal de la Empresa, dando permisos y restricciones a la información, hacia qué información debe conocer cada empleado y que no.
- Controlar el acceso a las páginas Web por los empleados, restringir ciertas páginas que pueden llamar la atención de los mismos, retardando así sus labores ocasionando pérdida de tiempo e impidiendo su labor eficiente dentro de la Empresa.
- La copia de seguridad de la base de datos debe hacerse de forma automática y no depender de una persona para realizar esta acción, evitando así el olvido de la misma, y mantener una mayor seguridad de la información.
- Implantar un Sistemas Multi agente para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY", que ayude a minimizar las vulnerabilidades y mantener un control adecuado de los empleados en sus respectivas labores.

CAPÍTULO VI

PROPUESTA

6.1. Datos informativos

- **TÍTULO**

"Sistemas Multi agente para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY"

- **INSTITUCIÓN EJECUTORA**

Empresa Importadora REPCOPY

- **DIRECTOR DE TESIS**

Ing. Clay Aldás

- **BENEFICIARIOS**

Empleados de la Empresa Importadora REPCOPY

- **UBICACIÓN**

Av. 12 de Noviembre 10-47 entre Tomas Sevilla y Espejo

- **TIEMPO ESTIMADO**

Fecha de Inicio: enero del 2012

Fecha de Finalización: Junio del 2012

- **EQUIPO TÉCNICO RESPONSABLE**
  - Investigador: William Pullutaxi
  - Gerente: José Luis Solano

6.2.Antecedentes de la propuesta

La tecnología informática avanza constantemente, por la cual hace imprescindible el estudio diario de nuevas herramientas que aparecen día a día y más aún cuando de proteger información de vital importancia para una Empresa se trata.

En la actualidad la Empresa no cuenta con una herramienta de seguridad que permita disminuir la vulnerabilidad de la red institucional

Es por ello que el factor humano ha tomado cada vez más un papel y posición muy importantes dentro del control de seguridad de la información de la Empresa, con el fin de que la información manejada dentro de la Empresa sea óptima y tenga un alto grado de confiabilidad, es por ello que se debe adoptar una política de seguridad en la Institución, para mejorar el nivel de acceso a la información así como también restringir ciertas páginas de Internet o a su vez realizar una seguimiento de las páginas accedidas por los usuarios para tomar una decisión adecuada que permita mejorar el rendimiento de las mismos.

Otra de las opciones viables es la implementación de un sistema de detección de intrusos que ayude a proteger la información y así disminuir la vulnerabilidad de la red de la Institución.

6.3.Justificación

La implantación de un sistema Multi-Agente se ha planteado con el objetivo de proponer un nuevo enfoque, que supere las limitaciones de los mecanismos de seguridad de la información existente utilizada en la detección de intrusiones en los entornos de aplicaciones Web de la Empresa Importadora REPCOPY.

Este sistema será de gran ayuda para brindar mayor seguridad de la información en la Empresa misma que resulta de la ejecución de las siguientes tareas.

- **Función Monitorización y Captura:** Encierra las tareas de monitorización del tráfico para identificar y capturar las peticiones de usuarios dirigidas a las aplicaciones.

- **Función de Clasificación Ligera:** Encierra las tareas correspondientes a la ejecución de un proceso rápido para detectar anomalías en las peticiones de usuarios.

- **Función de Clasificación Pesada:** Encierra las tareas correspondientes a la ejecución de un proceso exhaustivo para detectar anomalías en las peticiones de usuarios.

- **Función Administración:** Encierra las tareas relacionadas a la administración y control de la arquitectura así como también a la gestión de alertas y toma de decisiones frente a situaciones de amenazas.

6.4.Objetivos

6.4.1. Objetivo general

Implantar un sistema MULTI-AGENTE para reducir los ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY

6.4.2. Objetivos específicos

- Realizar un estudio de campo sobre los ataques más frecuentes en la Empresa.
- Determinar la realidad de la seguridad de la información en la misma.
- Establecer las herramientas necesarias para minimizar los ataques en la red.
- Implantar una herramienta de monitoreo detección de intrusos para minimizar el robo de información.

6.5.Análisis de factibilidad

- **Político**

El proyecto es factible para la ejecución porque en la Empresa brinda todas las facilidades para mejorar la seguridad de los sistemas de información que manejan y así brindar mayor confianza a todos los usuarios de la misma.

- **Socio cultural**

El uso de esta tecnología informática permitirá una mayor seguridad en la información que maneja cada una de las personas que laboran en la Institución brindando.

- **Tecnológico**

Para la implementación de este sistema la Institución cuenta con la infraestructura necesaria en redes de datos y sistemas de información, mismas que permitirán la implementación de un sistema que minimice las vulnerabilidades.

- **Equidad de género**

Este proyecto beneficiara a todo el personal que labora dentro de la Institución, protegiendo todos sus datos y haciendo de ellos más seguros y confiables.

- **Ambiental**

Para la implementación de este sistema Informático no será necesaria la utilización de substancias que pongan en peligro el medio ambiente.

- **Económico –financiero**

La Empresa cuenta con el factor financiero que ayude a la implementación del sistema informático para detectar intrusos en los diferentes entornos que manejan en la misma

- **Legal**

El proyecto está sujeto a todas las normas y leyes legales que el estado ecuatoriano lo dispone.

6.6.Fundamentación teórica

6.6.1. Vulnerabilidad en redes

Uno de los problemas de la red es precisamente la vulnerabilidad ya que cualquier persona con el conocimiento suficiente sobre redes, y una persona con terminal inalámbrico podría comunicarse con un punto de acceso privado si no se disponen de las medidas de seguridad adecuadas.

Dichas medidas van encaminadas en dos sentidos: por una parte está el cifrado de los datos que se transmiten y en otro plano, pero igual importante, se considera la autenticación entre los diversos usuarios de la red.

6.6.2. Principales ataques a las redes

Para localizar una máquina en la red es necesario conocer la dirección IP asignada por un servidor. Para tener acceso es necesario tener un puerto abierto. Por ejemplo, en el caso del acceso a la Web, por lo general, es necesario el puerto 8080 u 80 más

popularmente conocido y en el caso del acceso FTP (Protocolo de Transferencia de Archivos) necesitamos el puerto 21.

Por lo tanto, una vez conocido la dirección IP, es necesario escanear los puertos de la maquina cuya dirección conocemos. Estos programas varían de formato pero tienen como objeto en mismo fin.

Otro método de apertura de puertos es enviar al usuario un programa de despliegue un "Caballo de Troya" o "Troyano". Veamos un poco los diferentes tipos de ataques a redes y como funciona. Los ataques pasivos son aquellos donde un tercero no realiza ningún ataque, simplemente escucha. Los ataques activos, en cambio, buscan causar algún daño, como: perdida de confidencialidad, disponibilidad e integridad de información o sistema.

6.6.2.1.Ataques pasivos:

En los ataques pasivos el atacante no altera la comunicación, sólo la escucha o monitoriza, para obtener información. Por tanto este tipo de ataques suelen usar técnicas de escucha de paquetes (sniffing) y de análisis de tráfico. Son difíciles de detectar ya que no implican alteración de los datos. En algunos casos este tipo de ataques se pueden dificultar cifrando la información posible objetivo de escuchas. Con este ataque se busca obtener información que es normalmente transmitida por la red, como: usuarios, contraseñas, direcciones IP, etc. Este tipo de ataque es el más peligroso, ya que abre las puertas a otros paquetes.

6.6.2.2.Ataques activos:

Suponen alguna modificación del flujo de datos o la creación de flujos falsos. Hay muchas técnicas que se usan en este tipo de ataques. Ejemplos:

- **Suplantación:** el intruso se hace pasar por una entidad diferente, normalmente incluye alguna de las otras formas de ataque activo.
- **Modificación de mensajes:** Capturar paquetes para luego ser borrados (dropping attacks), manipulados, modificados (tagging attack) o reordenados
- **Re actuación:** Captura de paquetes y retransmisiones
- **Degradación:** Técnicas para que el servicio se degrade

6.6.3. Análisis de los ataques encontrados en la red de la Empresa REPCOPY

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.
Los ataques se producen en Internet, en su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo; en casos atípicos, son ejecutados por piratas informáticos. Para bloquear estas intrusiones es importante estar familiarizado con los principales tipos de ataques y tomar medidas preventivas.

Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema;
- Robar información (secretos industriales o propiedad intelectual)
- Recopilar información personal acerca de un usuario;
- Obtener información de cuentas bancarias u organización,
- Utilizar el sistema de un usuario como un "rebote" para un ataque;
- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

Una vez realizad la respectiva investigación de campo se ha logrado obtener información acerca de las anomalías a las que ha sido víctima la Empresa Importadora REPCOPY.

- **IP Spoofing:** El atacante cambia su dirección IP para poder pasar por alto controles de acceso.
- **Denial Of Services.** Este tipo de ataque busca dejar fuera de servicio a la red inalámbrica utilizando todo el ancho de banda para enviar paquetes basura
- **Ataques de Negación de Servicios** (DoS, por sus siglas en ingles). Ataques a una red diseñada para deshabilitarla mediante congestionamientos inútiles de tráfico. Muchos de estos ataques aprovechan las limitaciones de los protocolos TCP/IP. Existen métodos de reparación por software para todos los DoS conocidos que los administradores de sistemas pueden instalar para limitar los daños.
- **Troyano:** Programa destructivo que se encubre bajo la forma de una ampliación inofensiva. A diferencia de los virus, los troyanos no son capases de reproducirse por sí mismos, pero pueden ser igualmente destructivos.
- **Virus:** Todos los virus informáticos son diseñados por el hombre y muchos de ellos pueden reproducirse fácilmente.
- **Gusanos:** programa o algoritmo que se reproduce en una red informática y suele realizar actividades maliciosas, como consumir los recursos de la computadora y hasta cerrar el equipo.
- **Spam:** correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (en algunos casos de manera masiva) que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. La recepción de SPAM, o correo basura, se ha convertido en uno de los principales problemas de la comunicación por correo electrónico.

- **Amenazas del personal interno:** También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como "fisgones" en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización. Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno ("insiders") como con los usuarios externos del sistema informático ("outsiders").

Una vez expuesto una lista de ataques a las que está expuesto un equipo informático en general, pasamos a mostrar el siguiente cuadro con los ataques se presentan en la Empresa con los exploits utilizados.

ENTORNOS	CARACTERÍSTICAS	ATAQUES FRECUENTES	EXPLOITS SELECCIONADOS
Servidor	**Marca:** Intel **Procesador:** I7 de 3.7 GHZ **RAM: 4 GB** **Almacenamiento:** 4 discos de 1.5 TB total 6 TB Sistema Operativo: Windows server 2003 Service Pack 2	Contraseña nulas, Denioal of services (consumo de recursos) Utilización de Exploit, Obtención de password, Gusanos, Virus Troyanos, Spam, Suplantación de identidad, Robo de información Ataques de denegación de servicios (Inundación de conexiones, Ataque de vulnerabilidad (Puertos abiertos que no sean utilizados, etc))	windows/smb/ms08_067_netapi windows/http/novell_messenger_acceptlang windows/firewall/kerio_auth windows/browser/ms03_020_ie_objecttype
Estaciones de trabajos (Equipos de escritorio, portátiles)	**Marca:** Intel **Procesador**: Dual Core de 2.8 GHZ **RAM**: 2 GB **Almacenamiento:** 500 GB **Sistema Operativo :** Windows server xp Service Pack 2	Virus, Troyanos, Spam, Robo de contraseña, Suplantación de identidad, Copia de información no autorizada, Borrado, modificación o revelación desautorizada o inadvertida de información, Acceso físico no autorizado	windows/smb/ms08_067_netapi windows/ftp/32bitftp_list_reply windows/browser/ms03_020_ie_objecttype

Bases de Datos MySql 5.1	Gran rapidez y facilidad de uso Soporta gran cantidad de tipos de datos para las columnas Gestión de usuarios y passwords Infinidad de librerías y otras herramientas	Robo contraseña, mala manipulación de datos, errores personales.	windows/mssql/mssql_payload_sqli **(SQL injection).**
MicroPlus SQL	Sistema contable Cuneta con los siguientes módulos: Contabilidad Índices FinancierosCaja/Ingresos y Egresos (Cierres de Caja) Bancos / Conciliaciones Bancarias Ventas y Cuentas por Cobrar Compras y Cuentas por Pagar Bodega / Manejo de Inventarios SRI Anexos Transaccionales / REOC Nomina/Personal (Modulo Adicional) Producción (Formulación o Requisición de Materiales)	Suplantación de identidad Robo de contraseñas Acceso no autorizado al sistema Robo de información	
RED	Permite: Compartir archivos Compartir impresoras Compartir aplicaciones Servicio de correo electrónico Servicio de internet	Scaneos de puerto, Exploits, robo de contraseñas Denioal of service (consumo de ancho de banda, alteración de configuración de red, modificación de estados de servicios)	windows/http/altn_webadmin windows/ftp/easyfilesharing_pass windows/ftp/3cdaemon_ftp_user Sniffer (cain & abel) nmap

Tabla 20: Exploits utilizados para las vulnerabilidades de los equipos de la Empresa

Análisis:

Después de haber expuesto una lista de ataques a las que está sujeta los entornos de la Empresa, podemos darnos cuenta lo fácil que sería acceder a cualquier recurso, dando libertad a cualquier atacante de hacer y deshacer cualquier información.

Con un poco de investigación podemos encontrar muchas herramientas para aprovechar las vulnerabilidades que tienen los equipos de la red, para este caso hemos utilizados exploits para ingresar a una computadora.

Además existe la suplantación de identidad o lo que es lo mismo el robo de usuario y contraseña perjudicando a la Empresa realizando transacciones maliciosas en el sistema que maneja la Institución, causando perdida de mercadería y pérdidas económicas.

Otro de los problemas que hay que tomar énfasis es en la ingenuidad de las personas al momento de tomar su tiempo para almorzar, es decir que algunos usuarios dejan abierto el sistema de ventas con su respectivo usuario y contraseña haciendo de este un punto muy vulnerable y de fácil manipulación de la base de datos causando perdida de información.

Como podemos darnos cuenta, la falta de conocimiento en la gerencia, en el personal y la falta de capacitación sobre seguridad informática, es un punto que no está siendo tomado en cuenta, permitiendo que sigan dándose estas anomalías sin hacer nada al respecto.

También es necesario dar a conocer a los empleados que deben poner claves difíciles de descifrar, ya que en la Institución los usuarios mantienen claves como: fecha de nacimiento, número de teléfono, fecha de nacimiento de algún familiar, etc. Permitiendo que otras personas puedan dar con la clave y acceder al sistema informático y manipularlas de mala manera.

Otro punto importante que hay que considerar es que no cuentan con alguien capacito para que ayude a mejorar la protección de la red y por consiguiente a la protección de la información.

6.6.4. Seguridad en redes

Como sabemos, la seguridad en redes, es un factor muy importante debido a la naturaleza del medio de transmisión: cable, aire. Las características de seguridad de una red local, se basa especialmente en la protección a la comunicación entre el punto de acceso y los clientes, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

6.6.5. Sistemas de detección de intrusos

En este apartado se procederá a dar la explicación de las alternativas de solución para y posteriormente seleccionar un Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY.

6.6.6. Ventajas y desventajas de los IDS

Ventajas

Un IDS no impide la consecución de un ataque, pero permite alertar de su presencia. Las capacidades de éste permiten realizar actividades relacionadas con la seguridad informática como son las siguientes:

- Monitorización y análisis de las actividades de los usuarios. Como se ha descrito anteriormente, una gran proporción de los ataques informáticos son perpetrados por parte de los propios usuarios autorizados de la red. Un control

de sus actividades (respetando la intimidad de las personas) permite saber los servicios que utilizan y el uso que hacen de ellos.

- Auditoria de configuraciones y vulnerabilidades de sistemas. La detección de tráfico permite descubrir sistemas con servicios habilitados innecesarios o no autorizados, que de otra manera pasarían inadvertidos. El descubrimiento de una vulnerabilidad del sistema permite tomar medidas al respecto, eliminándola o si no es posible, poniendo especial atención en ella.
- Asegurar la integridad de los sistemas críticos. El análisis de tráfico permite saber si un determinado sistema ha sido atacado (o está en riesgo de ser atacado). De esta forma podemos estar seguros de que los sistemas están libres de ataques, ya que nunca se puede garantizar al 100% la eficacia de los cortafuegos.
- Análisis estadístico de ataques. Dado que la comparación de ataques contra una base de datos es algo limitada, existen herramientas heurísticas de búsqueda de patrones de ataques (como hacen los sistemas antivirus con el código malicioso). Sistemas basados en redes neuronales y demás métodos de inteligencia artificial se aplican cada vez con más frecuencia para este tipo de fines.
- Análisis de tráfico anormal. El tráfico autorizado que podemos considerar normal en nuestras funciones de negocio, puede dejar de serlo en determinadas circunstancias (conexiones fuera de las horas de trabajo, tráfico en segmentos de backup en estado de normalidad, accesos frecuentes a equipos de uso excepcional...).
- Auditorias del entorno. Tras un cortafuego es una excelente herramienta para determinar qué tipos de ataques pasan a través del cortafuego (y así comprobar su funcionamiento) y cuáles de ellos tienen éxito (y así comprobar la eficacia de los elementos menores de seguridad: cortafuegos de host y Antivirus).

Desventajas

Las ventajas del uso junto a un cortafuego adecuadamente configurado son claras, y se ha hecho hincapié en ellas. Pero tienen también grandes desventajas, que se deben tener en cuenta para no confiar excesivamente en ellos:

- No puede hacer nada frente a ataques nuevos y que por tanto es incapaz de reconocer como tales. La actualización de la base de reglas de reconocimiento de patrones es una importante actividad rutinaria de su mantenimiento.
- No puede detectar ataques en comunicaciones cifradas extremo-extremo, ya que es incapaz de reconocer patrones en un contenido ilegible.
- No puede compensar mecanismos de autenticación débiles. Si es sencillo obtener usuarios y claves legales y acceder con ellos al sistema, el IDS será incapaz de alertar del acceso no autorizado.
- No puede automatizar la investigación de los incidentes. Es necesaria la intervención humana (de un analista cualificado) para descubrir la naturaleza real del ataque, limpiar sus efectos, descubrir al atacante y protegerse para el futuro.
- Mal configurado puede dar lugar a errores y confusiones típicas de este tipo de sistemas:
    - Falsos positivos: Alertas disparadas en condiciones normales. Este tipo de situación es indeseable, debido a que hace que el administrador de red se alarme innecesariamente y termine por ignorar alertas reales pensando que se trata de este tipo de errores. Esta situación se da en IDS configurados con excesivo nivel de detalle y propensos a alertar de la más mínima variación respecto a la normalidad.
    - Falsos negativos: Ausencia de alertas en condiciones de ataque y tráfico no autorizado. Este tipo de error es peor que el anterior, ya que el IDS no realiza su función de avisar de la situación, lo que implica que el ataque pase desapercibido y por tanto, no se tomen medidas adecuadas y eficaces a tiempo de evitar males mayores.

6.6.7. Tipos de sistemas de detección de intrusos.

Existen tres tipos básicos de IDS según el fin para el cual están diseñados [KOZI03]:

- **Network Intrusión Detección System (NIDS):** Son instalados en un segmento de red en concreto, del cual pueden absorber todo el tráfico (escuchan en modo promiscuo) y analizarlo en tiempo real para disparar las alertas correspondientes. Cuanto más transparente sea su funcionamiento y menos interfiera en el tráfico de red mejor.

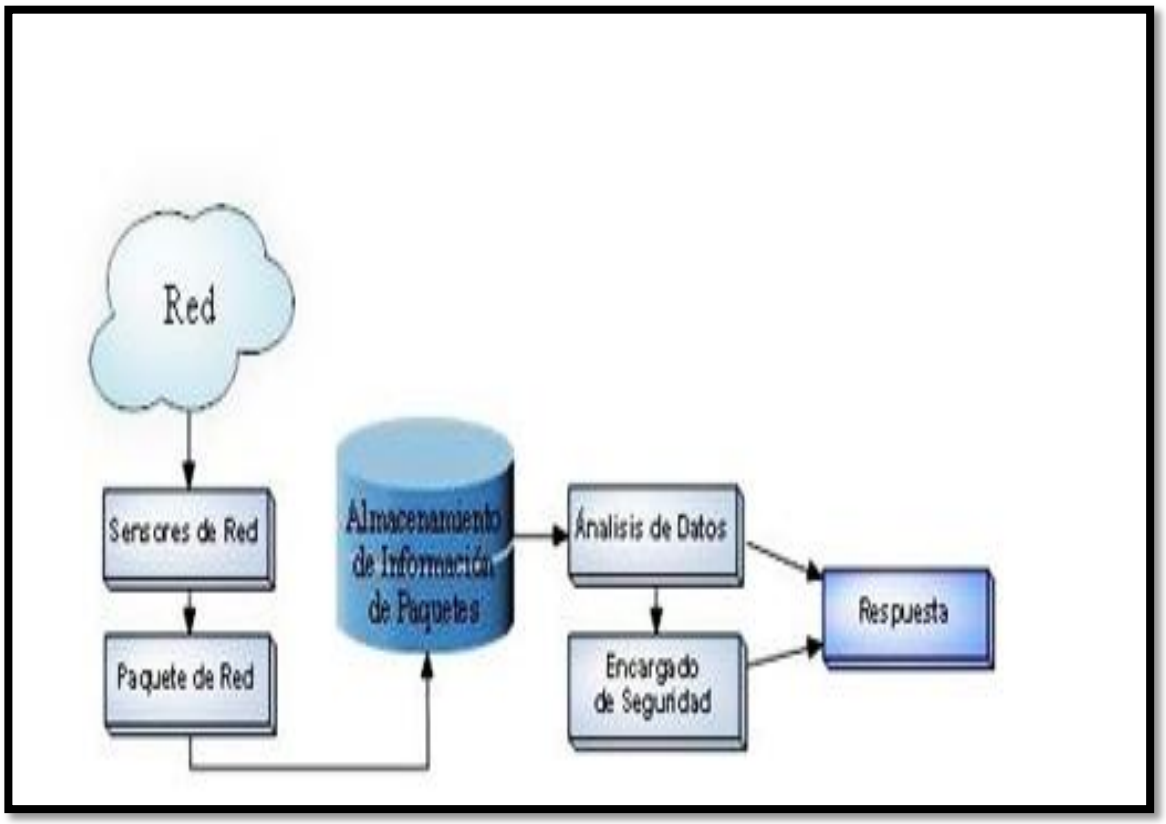


Figura 21: Network Intrusión Detección System (NIDS)

Autor: María Isabel Giménez García, Almería 2008

- **Network Node Intrusión Detección System (NNIDS):** Son instalados en un host en concreto, analizando todo el tráfico destinado a dicho equipo. Se suelen utilizar sobre equipos críticos de la compañía propensos a ser objetivo

de ataques o en un HoneyPot (host débilmente protegido que sirve de trampa para hackers desviando su atención de los equipos más importantes).

- **Host Intrusión Detección System (HIDS):** Son instalados en un host en concreto y permiten tomar una instantánea del sistema, para comprobar más adelante la integridad de la máquina. La diferencia con los NNIDS es que no tienen en cuenta las comunicaciones, sino que buscan rastros de un ataque en el propio equipo. Permiten saber si un ataque ha tenido éxito y cuales han sido las consecuencias a posteriori.

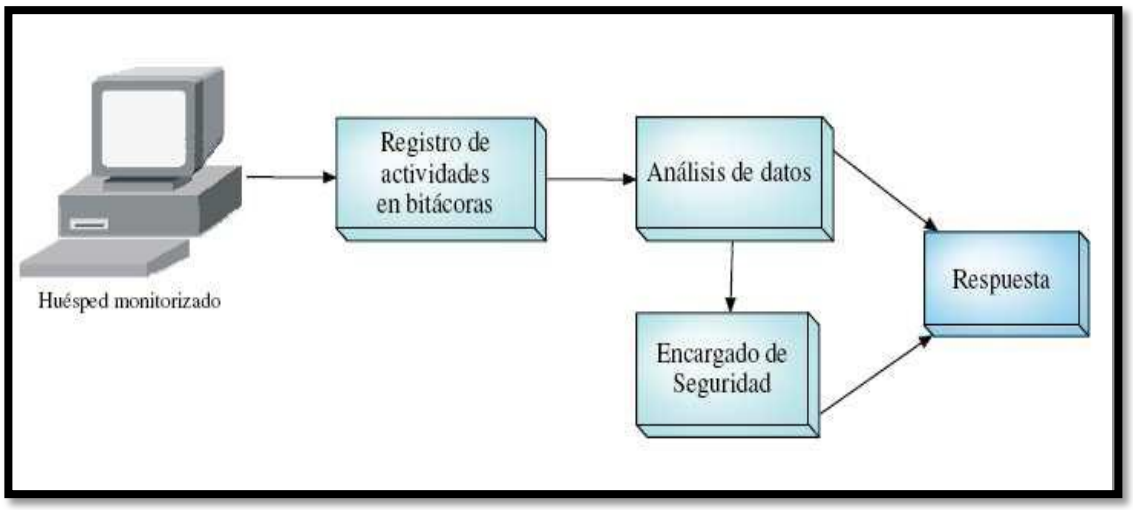


Figura 22: Host Intrusión Detección System (HIDS)

Autor: María Isabel Giménez García, Almería 2008

Los IDS también se pueden clasificar en las siguientes categorías según su forma de detectar las intrusiones:

- **Búsqueda de patrones (Signature detection):** Los IDS de este tipo disponen de una base de datos que contiene patrones o firmas de ataques conocidos, y cada paquete que se analiza se contrasta con esa base de conocimiento. Cuanto mayor sea la lista de firmas conocidas, mas tipos de ataques se podrán detectar, pero más costoso computacionalmente será para cada paquete,

pudiéndose perder alguno si el ritmo de análisis no soporta el del flujo de información.

- **Análisis de tráfico (Anomaly detection):** Los IDS de este tipo están configurados para conocer la situación "normal" de la red. Recolectan todo el tráfico y crean estadísticas en tiempo real del estado de la red. Si en un momento determinado, la estadística se sale de la normalidad, se genera la alerta para que el analista lo investigue.
- **Verificación de integridad:** Es el sistema que utilizan los HIDS. Se comprueban determinados aspectos de un equipo (checksum de ficheros críticos, registro del sistema, logs...). Permite saber a posteriori, que tipos de ataques se han perpetrado en un sistema y los danos que han producido.

6.6.8. Implantación de IDS

Hasta este punto se ha pretendido dar una visión general de los IDS: sus funcionalidades, utilidad, ventajas e inconvenientes. Un IDS es un dispositivo que complementa las medidas de seguridad de la red, muy útil para tomar medidas concretas frente a una situación de crisis, e incluso para poder preverla. Este punto hace hincapié en la dificultad que conlleva el uso de este tipo de dispositivos, desde la necesidad de conocimientos avanzados de seguridad para configurarlos correctamente y saber interpretar sus alertas hasta la experiencia necesaria en seguridad perimetral para saber ubicarlos en la red de forma que den un resultado eficaz.

6.6.9. Pasos a seguir para la implantación de un IDS de forma eficiente

6.6.9.1.Identificación de necesidades de la Empresa

Se debe determinar la importancia de la información. Cuantificar en términos económicos y subjetivos (confianza pública en la compañía, respeto por parte de otras

Empresas...) las perdidas en que se incurriría si los datos se perdieran y/o fueran robados. Esta cuantificación permitirá valorar si resulta rentable implantar el sistema o no y determinar la probabilidad de sufrir un ataque por parte de un hacker interesado en obtener beneficio. Si la red ya ha estado bajo ataque anteriormente, se conocen sus vulnerabilidades y ha mostrado signos de debilidad es probable que pueda volver a sufrir un ataque. Determinar el nivel de seguridad a implantar en la red es necesario para establecer un plan de seguridad concreto.

6.6.9.2.Obtener conocimientos sobre la detección de intrusos

Es necesario tener unas nociones básicas de lo que puede hacer un IDS y para qué sirve, o de lo contrarios tendría una falsa ilusión de seguridad. El conocimiento sobre ataques informáticos y sobre el estado del arte en temas de seguridad es fundamental para poder interpretar adecuadamente los resultados del IDS.

6.6.9.3.Obtener conocimientos sobre la infraestructura de red empresarial

Una red debidamente estructurada en diferentes segmentos protegidos con cortafuegos es más segura que una mal administrada. La distribución de sensores en las diferentes subredes dará lugar a una variedad más rica y precisa de análisis.

6.6.9.4.Escoger el IDS más adecuado

Se debe elegir el sistema IDS que mejor se ajuste a las necesidades de protección de la red, condicionado su complejidad al nivel de conocimiento por parte del administrador/analista. Evaluar varios IDS simulando baterías de ataques en un entorno de pruebas similar a la red sobre la que implantar definitivamente el producto requiere trabajo y una gran pericia, pero es el mejor método para decantarse por un IDS en particular.

6.6.9.5.Especificar una política de seguridad:

Es fundamental contar con un protocolo de actuación concreto frente a una situación de alerta por parte del IDS, ya que de nada sirve ser capaz de detectar ataques si luego

no se sabe qué hacer en respuesta. Debe contarse con una documentación completa sobre lo que hacer en cada situación, de forma que no surjan dudas sobre el plan de acción. Esta documentación es específica de cada organización y no es trivial realizarla, por lo que debe ser creada por expertos en seguridad y planes de emergencia. El administrador de red encargado de seguir esta política también deberá tener conocimientos avanzados de este tipo para poder intervenir rápida y eficazmente sin dudar en ninguna situación.

6.6.10. Acciones que un administrador de red puede llevar a cabo para ajustar un IDS.

- **Optimizar la base de datos de firmas**: En general, la configuración por defecto de los IDS busca todos los ataques conocidos posibles. Es importante conocer bien la red que se pretende administrar para no perder tiempo de CPU chequeando firmas de ataques que nunca tendrían éxito en nuestra configuración.
- **Filtrar tráfico no deseado:** Por defecto, el IDS analiza todo el tráfico que es capaz de capturar en su segmento de red, al igual que puede identificar firmas en tráficos cifrados.
- **Balanceo de carga**: Al ser un IDS un dispositivo computacionalmente pesado, si el volumen de tráfico a analizar es muy importante, es recomendable la instalación de varios sensores balanceados por tipo de tráfico. Reduciendo el número de reglas que se comparan en cada sensor se obtiene un mejor rendimiento por cada uno, pero hay que cuidarse de no dejar reglas relevantes sin supervisar.

6.6.11. Soluciones existentes de software IDS

A continuación se muestra un cuadro con la lista de los IDS y una breve descripción de su funcionamiento.

SOFTWARE	TECNOLOGÍA	ALCANCE	RESPUESTA	TIEMPO	PROTOCOLOS QUE SOPORTA	SISTEMAS OPERATIVOS	CARACTERÍSTICAS
SNORT	Monitorización de red	Red	Pasiva	On-line	TCP/IP (Ethernet, SLIP, PPP y ATM)	Windows/Linux	Utiliza plugins para grabar ataques de: (SQL , tcpdump , archivo de texto, XML, syslog , SMB)
EMERALD	Monitor de eventos	Nodo y Red	Pasiva	0n-line	Ethernet	Windows /Linux	Es una herramienta para analizar y evaluar los inpactos de las normas de seguridad, evaluación de riesgos y establecer normas de seguridad tanto de la red interna como del internet.
PANDORA FMS	Monitorización de red	Nodo y red	Pasiva	On-line	Telnet, Ftp, ICMP	Windows/ Linux	Permite la monitorización remota de (WMI, SNMP, TCP. UDP, ICMP, HTTP)
WIRESHARK	Monitorización de red	Nodo y red	Pasiva	On-line	Telnet, Ftp	Windows/ Linux	Se utiliza para la red de resolución de problemas, análisis, software y comunicaciones de protocolo de desarrollo

Tabla 21: Características de los IDS estudiados

Autor: William Pullutaxi

6.6.12.1.Snort

Es un IDS en tiempo real desarrollado por Martín Roesch y disponible bajo GPL. Se pueden ejecutar en máquinas con sistemas operativos UNIX y WINDOWS. Es uno de los sistemas de detección de intrusos en este momento.

En un principio fue diseñado para cumplir los requerimientos de un IDS Ligero. Era pequeño y flexible, pero poco a poco ha ido creciendo e incorporando funcionalidades que solo estaban presentes en los IDSs comerciales.

En Snort no es posible separar el componente de análisis y los sensores en máquinas distintas, la arquitectura Snort se enfocó para ser eficiente, simple y flexible. Snort está formado por tres sistemas: el decodificador de paquetes, la máquina de detección y el subsistema de alertas y logs.

- **Decodificador de paquetes**

Soporta gran variedad de protocolos de capa de enlace TCP/IP, tales como Ethernet, SLIP, PPP y ATM. Cada subrutina del decodificador ordena de una forma distinta los paquetes, formando una estructura de datos basados en punteros por encima del tráfico real capturado. Esta estructura de datos será la que guie al motor de análisis para el posterior análisis.

- **Motor de detección**

Snort mantiene sus reglas de detección en una lista enlazada bidimensional. La lista base se denomina “Chain Header” y la que se deriva de esta se llama “Chain Option”. Cuando llegue un paquete al motor de detección, este busca en la lista “Chain Header” de izquierda a derecha la primera coincidencia. Después, buscara por la lista “Chain Option” si el paquete cumple las opciones específicas.

- **Subsistemas de alertas y log**

Actualmente hay tres sistemas de log y cuatro de alerta. Las opciones de log pueden ser actividades para almacenar paquetes en forma decodificada y entendible por humanos o en formatos tcdump. Avisan del tipo de ataque detectado y ofrece

información adicional como ip origen y destino, fecha y hora de la detección y campo de datos. Snort dispone de un mecanismo que optimiza considerablemente su rendimiento. Puesto que normalmente se requiere de un sistema back-end potente como una base de datos SQL para hacer correlaciónales de los ataques, las estructuras de los logs suelen ser muy costosas. Al ser Snort un proceso monolítico, mientras que se encuentra escribiendo en la base de datos es incapaz de hacer otras cosas, como procesar el tráfico de entrada. Lógicamente estos procesos necesitan comunicarse, pero esta comunicación esta optimizada para que sea muy rápida que la estructura en una base de datos compleja como puede ser Oracle o MS-SQL.

6.6.12.2.Emerald

EMERALD (Event monitoring enabling responses to anomalous live disturbances) es un framework para efectuar deteccion de intrusos escalable, distribuida e inter operable a nivel de host y a nivel de red. Más que un IDS, es una propuesta de arquitectura para un IDS, que se supone debe contener componentes que permitan al sistema responder activamente ante amenazas, principalmente de ataques externos a una organización, aunque no se excluye la detección de ataques internos.

La arquitectura de EMERALD está compuesta de una colección inter operable de unidades de análisis y respuestas llamadas “monitores”, que ofrecen una protección localizada de activos claves dentro de una red corporativa. Al implantar monitores localmente, EMERALD ayuda a reducir las posibles demoras en análisis y respuesta que podrían ser consecuencia de la topología especialmente distribuida de una red.

Adicionalmente, introduce un esquema de análisis compuesto, en donde los análisis locales son compartidos y correlacionados en las capas más altas.

La arquitectura de EMERAL pretende ser pequeña y rápida, y lo suficientemente general para ser implantada en cualquier capa dentro de su esquema jerárquico de análisis. Los monitores incorporan un API versátil que mejora su habilidad para inter operar con la maquina objeto del análisis y con otros IDS.

6.6.12.3.Wireshark

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix.
Conocido originalmente como Ethereal, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.
Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados.

WireShark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú Statistics que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Podemos distinguir entre cada una de las anteriores:

- Estadísticas Generales
    - Summary, la cantidad de paquetes capturados.
    - Protocol Hierarchy, presenta las estadísticas para cada protocolo de forma jerárquica.
    - Conversations, un caso particular es el tráfico entre una IP origen y una IP destino.
    - Endpoints, muestra las estadísticas de los paquetes hacia y desde una dirección IP.
    - IO Graphs, muestra las estadísticas en grafos.
- Estadísticas específicas de los protocolos
    - Service Response Time entre la solicitud (request) y la entrega (response) de algún protocolo existente, entre otras.

6.6.12.4. Pandora FMS

Pandora FMS es capaz de detectar una interfaz de red que se ha caído, así como el movimiento de cualquier valor del NASDAQ. Si es necesario, Pandora FMS puede enviar un mensaje SMS cuando falle cualquier sistema o aplicación.
Pandora FMS permite conocer el estado de cualquier elemento de sus sistemas de negocio. Pandora FMS vigila su hardware, su software, sus aplicaciones y por supuesto, su Sistema Operativo. Pandora FMS es capaz de detectar una interfaz de red que se ha caído, así como el movimiento de cualquier valor del NASDAQ.

6.6.13 Backtrac 5 herramienta de ataque implementada

Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se ha convertido en una distribución de culto para los profesionales de la seguridad informática, cada versión que nos regalan sus desarrolladores, es esperada con ansias por una comunidad cada vez más grande de interesados por la seguridad de la información y esta historia se repite con cada nueva entrega de Backtrack

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanner de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless

Entre las nuevas características destacan:

- Ahora *BackTrack 5* incluye nativamente los gestores de ventanas Gnome, KDE y Fluxbox
- Soporte para arquitecturas de 32 y 64 bits, ARM: Facilitando el análisis forense y la posibilidad de ejecutarlo en dispositivos móviles.

- Backtrack 5 ahora es completamente Open Source: Aunque BackTrack está basado en proyectos open source, muchos de los cambios que han realizado sobre ellos no se habían publicado… hasta ahora, además aseguran que siempre será así.
- En esta nueva versión de Backtrack 5, se ha reorganizado el menú para facilitar su uso y cumplir los estándares, además actualizaron todas las herramientas.

6.6.14 Selección y justificación del Sistema de detección de ataques

Luego de haber realizado el análisis respectivo de acuerdo a las necesidades de la Empresa se ha seleccionado el software **PANDORA FMS**, por las siguientes razones:

- Pandora FMS recoge datos de cualquier sistema.
- Genera alarmas.
- Integra herramienta de monitorización que no sólo mide si un parámetro está bien o mal.
- Permite cuantificar el estado (bien o mal) o almacenar un valor (numérico o alfanumérico) durante meses si es necesario
- Permite medir rendimientos, comparar valores entre diferentes sistemas y establecer alertas sobre umbrales.
- Trabaja sobre una base de datos de forma que puede generar informes, estadísticas, niveles de adecuación de servicio (sla) y medir cualquier cosa que proporcione o devuelva un dato.
- Puede medir cualquier cosa: sistemas operativos, servidores, aplicaciones y sistemas hardware tal como cortafuegos, proxis, bases de datos, servidores Web, vpn, routers, switches, procesos, servicios, acceso remoto a servidores, etc.

6.6.14.1.Requisitos mínimos de Hardware

Los requisitos para la consola y el servidor de pandora son:

- 2GB de RAM y una CPU de un sólo núcleo a 2GHz de reloj. Disco duro rápido, 7200rpm o equivalente.
- 4GB de RAM y una CPU de doble núcleo a 2.5GHz de reloj y disco duro rápido (7.200 rpm o más)
- 12GB de RAM, una CPU con cuatro núcleos a 3GHZ y disco duro muy rápido (15.000 rpm o más).

Estos requisitos pueden variar dependiendo del número de máquinas o agentes que se instale en la red.

6.6.14.2.Requisitos Mínimos de software

- **Requisitos para el agente**

El agente puede ejecutarse en cualquier hardware que pueda ejecutar el sistema operativo mínimo requerido, siendo:

- Windows 2000 SP3
- Windows 2003
- Windows XP
- Windows Vista
- Windows 7
- Windows 2008
- SUSE Linux 10
- Ubuntu Linux 8.04
- Debian Linux
- Solaris 2.6

Se sabe que el agente se ha ejecutado con éxito en otros sistemas operativos anteriores, pero no existe soporte oficial. El agente no funciona en Windows NT4. Para monitorizar sistemas Windows, se puede instalar un entorno Cygwin e instalar el agente para Linux, aunque el rendimiento es muy inferior al de un agente nativo Windows.

- **Requisitos para el servidor**

Aunque puede trabajar sobre cualquier sistema operativo con Perl 5.8 instalado y con iThreads habilitados, se recomienda y está soportado únicamente sobre

Linux, siendo las distribuciones recomendadas SUSE (SLES u OpenSuse) y Ubuntu/Debian. Algunas personas lo tienen funcionando bajo sistemas BSD y sobre sistemas Solaris.

Hay que destacar que Pandora FMS necesita un servidor MySQL para almacenar toda la información. Este servidor puede instalarse en cualquier plataforma soportada por MySQL (Windows, Linux, Solaris, etc).

Se deberá tener instalado Perl 5.8, al menos, para que el servidor funcione correctamente. Además de los paquetes de SNMP del sistema operativo (netsnmp) para usar el servicio SNMP de Pandora FMS. También se requiere una base de datos (MySQL). También se requieren los paquetes nmap y opcionalmente el paquete xprobe2 para utilizar las características avanzadas de reconserver, así como las bibliotecas traceroute de Perl para poder hacer autodescubrimientos de red. Por último, también es necesario, el cliente binario de WMI para hacer consultas WMI contra sistemas Windows. Dicho cliente binario es parte del proyecto SAMBA (v4) y puede ser compilado no sin cierta dificultad en cualquier entorno Unix.

- **Requisitos para la consola**

De igual manera que el servidor, se recomienda su operación sobre sistemas Linux, pero dado que la interfaz Web es una aplicación AMP pura (Apache, MySQL y PHP), podría trabajar teóricamente sobre cualquier sistema que lo soporte: Windows, Unix, etc.

- **Requisitos para administrar la herramienta vía WEB**

Se deberá disponer de un navegador Web para instalar y comprobar el funcionamiento de la consola. En principio no se requiere que el navegador tenga el complemento de FLASH instalado, aunque se recomienda para poder hacer uso de las gráficas interactivas en Flash, para esto puede utilizar Internet Explores, Mozilla entre otros navegadores.

- **Dependencias de paquetes**

  Pandora FMS depende en gran parte del sistema operativo Linux, pero además necesita paquetes adicionales que muchas veces no vienen instalados de forma predeterminada. En el proceso de instalación se detallan de forma específica esas dependencias para sistemas Debian/Ubuntu y OpenSUSE.

6.6.14.3.Introducción a Pandora FMS

Es un proyecto OpenSource liderado por Ártica, Empresa española fundada en 2005, tiene una activa comunidad de miles de Empresas y más de 450.000 descargas.

Se utiliza en cinco continentes en más de 75 países diferentes es una aplicación de monitorización para vigilar todo tipo de sistemas y aplicaciones. Pandora FMS permite conocer el estado de cualquier elemento de sus sistemas de negocio. Pandora FMS vigila su hardware, su software, sus aplicaciones y por supuesto, su Sistema Operativo. Pandora FMS es capaz de detectar una interfaz de red que se ha caído, así como el movimiento de cualquier valor del NASDAQ. Si es necesario, Pandora FMS puede enviar un mensaje SMS cuando falle cualquier sistema o aplicación.

Este software interesa a todos aquellos que trabajan como administradores de red cuyo objetivo es precautelar la información que manejan dentro de una Institución, así como también asegurarse que los sistemas informáticos funcionen de la mejor manera y esté disponible en el momento que lo requieran.

6.6.14.4.Historia

Pandora FMS ha venido evolucionando de manera constante, debido a las necesidades que día a día van apareciendo dentro de una Institución, mismos que son tomados en cuenta por los diseñadores de este sistema y mejoran las versiones futuras que tomen en cuenta estas necesidades y cada vez sea un sistema eficiente a la hora de monitorear los equipos de cómputo y la red.

A continuación se mostrara un gráfico de la notable evolución que ha sufrido desde su aparición hasta el día de hoy.

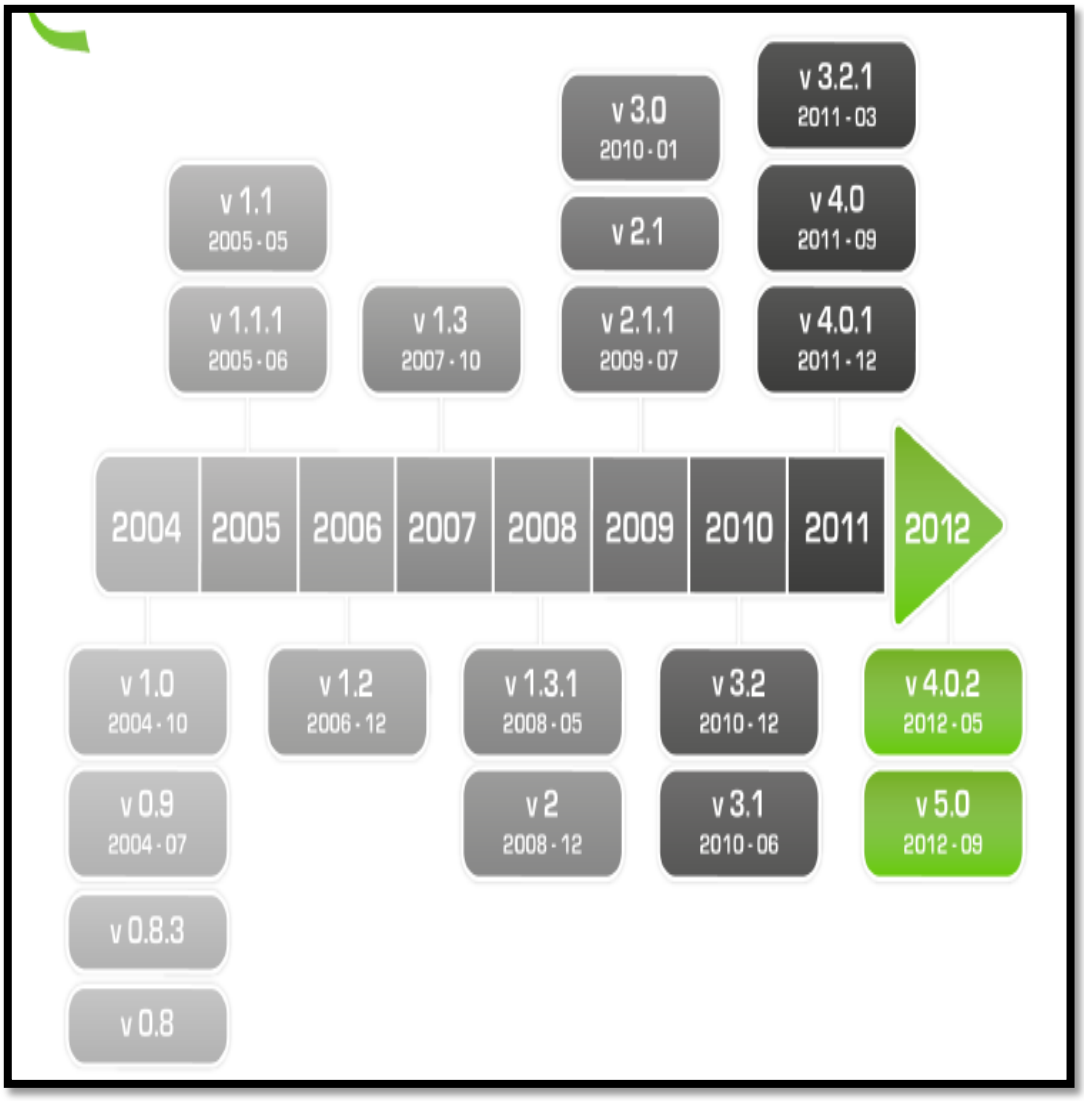


Figura 23: Evolución de Pandora FMS

Fuente: http://pandoraFMS.com/pandora/doc/es

6.6.14.5. Arquitectura de Pandora FMS

Pandora FMS es extremadamente modular y descentralizada. El componente más vital y donde se almacena todo es la base de datos (actualmente sólo se soporta MySQL). Todos los componentes de Pandora FMS se pueden replicar y funcionar en un entorno de HA puro (Activo/Pasivo) o en un entorno clusterizado (Activo/Activo con balanceo de carga).

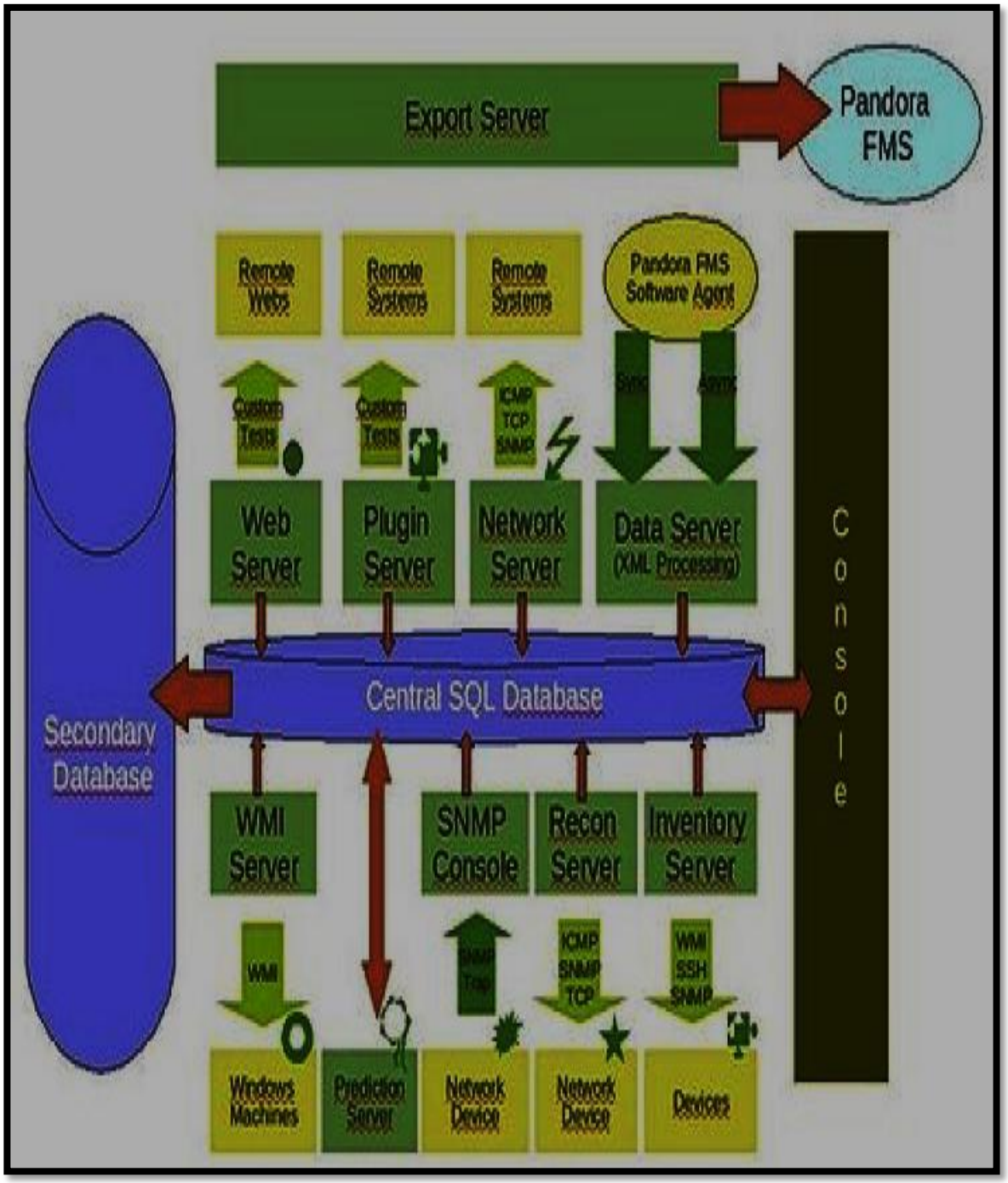


Figura 24: Arquitectura de Pandora FMS

Fuente: http://pandoraFMS.com/pandora/doc/es

A continuación se detallara todos los componentes:

- **Servidores de Pandora FMS**

Los servidores de Pandora FMS son los elementos encargados de realizar las comprobaciones existentes. Ellos las verifican y cambian el estado de las mismas en función de los resultados obtenidos. También son los encargados de disparar las alertas que se establezcan para controlar el estado de los datos.

Los servidores de Pandora FMS están siempre en funcionamiento y verifican permanentemente si algún elemento tiene algún problema y si está definido como alerta. Si ocurre esto, éste ejecuta la acción definida en la alarma, tal como enviar un SMS, un correo electrónico, o activar la ejecución de un script.

Pandora FMS gestiona automáticamente el estado de cada servidor, su nivel de carga y otros parámetros. El usuario puede monitorizar el estado de cada servidor, a través de la sección de estado de servidores de la consola Web.

  - **Servidor de datos**

    Procesa la información enviada por los agentes Software. Los agentes Software envían los datos XML al servidor por medio de diferentes formas de envío (FTP, SSH, o Tentacle) y el servidor verifica periódicamente si tiene nuevos ficheros de datos esperando a ser procesados. Este proceso utiliza un directorio del disco como "cola" de elementos a procesar.

    Se pueden instalar diferentes servidores de datos en diferentes sistemas o en el mismo anfitrión (que serán diferentes servidores virtuales). Varios servidores pueden trabajar juntos para entornos muy extensos y que necesiten aprovechar mejor el.

    El servidor de datos como el resto de servidores accede a la base de datos de Pandora FMS, que se comparte con el servidor Web, y que almacena los paquetes de datos procesados.

    A pesar de su sencillez y escasa utilización de recursos, el servidor de datos es uno de los elementos críticos del sistema, ya que procesa toda la información de los agentes y genera alertas y eventos del sistema

conforme a esos datos. El servidor de datos sólo trabaja con los datos que llegan en XML desde los agentes software y no realiza ningún tipo de comprobación remota.

- **Servidor de red**

Ejecuta tareas de monitorización remota a través de la red: pruebas ICMP (Ping, tiempos de latencia), peticiones TCP y peticiones SNMP. Cuando se asigna un agente a un servidor, se está asignando a un servidor de red, no a un servidor de datos, así que es muy importante que las máquinas que ejecutan los servidores de red tengan «visibilidad de red» para poder ejecutar las tareas de monitorización de red asignadas a los mismos. Es decir, que si va a hacer pings a sistemas de una red determinada, el servidor de red pueda llegar a esa red:

Por ejemplo, si se crea un módulo para hacer una comprobación de ping a 192.168.1.1 y se asigna este agente/módulo a un servidor en una red 192.168.2.0/24 sin acceso a la red 192.168.1.0/24 siempre devolverá DOWN ya que no puede contactar con ella.

- **Servidor de SNMP (también conocida como Consola de Traps SNMP)**

Este servidor utiliza el demonio standard del sistema de recolección de traps, snmptradp. Este demonio recibe traps SNMP y el servidor SNMP de Pandora FMS los procesa y almacena en la base de datos. Cuando los procesa y analiza, también puede lanzar las alertas asignadas en la consola SNMP de la consola de Pandora FMS.

- **Servidor de WMI**

WMI es un estándar de Microsoft para obtener información del sistema operativo y aplicaciones de entornos Microsoft Windows. Pandora FMS tiene un servidor dedicado para realizar llamadas nativas WMI de forma

centralizada. Con él se pueden recoger datos de sistemas Windows de forma remota, sin agente.

- **Servidor de reconocimiento**

Utilizado para explorar regularmente la red y detectar nuevos sistemas en funcionamiento. El servidor recon también puede aplicar una plantilla de monitorización para aquellos sistemas detectados recientemente y aplicar automáticamente los módulos por defecto definidos en esa plantilla para que se puedan utilizar para monitorizar inmediatamente el nuevo sistema. Utilizando las aplicaciones de sistema nmap, xprobe y traceroute es capaz además de identificar sistemas por su Sistema Operativo, en función de los puertos que tenga abiertos y establecer la topología de red en función de los sistemas que ya conoce.

- **Servidor de complementos (Plugins)**

Realiza comprobaciones complejas de usuario desarrolladas en cualquier lenguaje e integrados en la interfaz de Pandora FMS y gestionados de forma centralizada. Esto permite a un usuario avanzado definir sus propias pruebas complejas, desarrolladas por el mismo, e integrarlas en la aplicación para que se puedan usar de forma cómoda y centralizada desde Pandora FMS.

- **Servidor de predicción**

Es un pequeño componente de Inteligencia Artificial que implementa de forma estadística una previsión de datos en base a datos pasados con una profundidad de hasta 30 días en cuatro referencias temporales y que permite predecir los valores de un dato con un intervalo de 1015 minutos, y conocer si un dato en el momento actual es anómalo respecto a su historial. Básicamente usted tendrá que construir una baseline dinámica con un perfil semanal.

- **Servidor de pruebas WEB (Goliat)**

(Sólo versión Enterprise)

El servidor de pruebas WEB sirve para hacer pruebas de carga. Realiza comprobaciones WEB sintéticas, esto es, comprobaciones Web completas, desde el proceso de identificación de un usuario, pasó de parámetros por formulario, comprobación de contenidos, navegación por menús, etc. Se utiliza para pruebas de comprobación (funciona, no funciona) y para obtener tiempos de latencia de experiencia completa de navegación (incluyendo recursos asociados a la página (imágenes, textos completos, etc).

- **Servidor de exportación**

(Sólo versión Enterprise)

El servidor de exportación de Pandora FMS permite exportar los datos de un dispositivo monitorizado de una instalación de Pandora FMS a otra, y así tener replicados los datos. Esto es especialmente útil cuando se tiene una gran despliegue, con varias instalaciones de Pandora FMS, y se quiere tener cierta información crítica centralizada en uno sólo.

- **Servidor de inventario**

(Sólo versión Enterprise)

El servidor de inventario obtiene y visualiza información de inventario de los sistemas: Software instalado, parches instalados, chips de memoria en el hardware, discos duros, servicios corriendo en el sistema, etc. Puede obtener esta información tanto de forma remota como de forma local, a través de los Agentes Software.

- **Consola Web de Pandora FMS**

Es la interfaz de usuario de Pandora FMS. Esta consola de administración y operación permite a diferentes usuarios, con diferentes privilegios, controlar el

estado de los agentes, ver información estadística, generar gráficas y tablas de datos así como gestionar incidencias con su sistema integrado. También es capaz de generar informes y definir de forma centralizada nuevos módulos, agentes, alertas y crear otros usuarios y perfiles. La consola Web está programada en PHP y no requiere por parte del usuario final la instalación de ningún software adicional: ni Java, ni ActiveX. No obstante, las gráficas también están disponibles en FLASH y para poder verlas en este formato será necesario el complemento de FLASH para su navegador; puede accederse desde cualquier plataforma moderna que soporte HTML y CSS. Se recomienda Firefox 2.x o IE 7.x. La experiencia de usuario con navegadores como IE6 es muy pobre, y se pierden la mayoría de las ventajas implementadas en la Consola WEB de Pandora FMS 3.0

La consola Web a su vez, puede ejecutarse en múltiples servidores, esto es, podemos tener tantas consolas Web como queramos, tanto para repartir carga como para facilitar el acceso por problemas logísticos (grandes redes, numerosos grupos de usuarios diferentes, diferencias geográficas, diferencias administrativas, etc.). Su único requisito es poder acceder al contenedor de datos donde Pandora FMS almacena todo: la base de datos y en el caso de la versión enterprise, acceder al repositorio de configuraciones de los agentes de forma sincronizada (via NFS).

- **Base de datos de Pandora FMS**

Pandora FMS utiliza una base de datos MySQL. Pandora FMS mantiene una base de datos asíncrona con todos los datos recibidos, realizando una cohesión temporal de todo lo que recibe y normalizando todos los datos de las diversas fuentes origen. Cada módulo de datos de cada agente genera una entrada de datos para cada paquete, lo que supone que un sistema real de producción puede tener del orden de diez millones de «datos», o átomos de información.

Estos datos se gestionan automáticamente desde Pandora FMS, llevando a cabo un mantenimiento periódico y automático de la base de datos, esto permite que Pandora FMS no requiera ningún tipo de administración de base de datos ni proceso manual asistido por un operador o administrador.

Esto se realiza por medio de una purga periódica de los datos pasada una fecha (90 días de forma predeterminada), así como una compactación de los datos que tienen más de un número determinado y configurable de días de antigüedad (30 días de forma predeterminada).

- **Agentes Software de Pandora FMS**

Cuando nos referimos a un agente en Pandora FMS, podemos hacer referencia a tres piezas fundamentales en la recolección de datos:

- Agente
- Agente Software (Aplicación software, Pandora FMS Agent, que corre en una máquina).
- Agente Físicos (hardware)

Agente

El agente de Pandora FMS, "a secas" es simplemente un elemento organizativo creado con la consola Web de Pandora FMS y que está asociado a un grupo de módulos (o elementos individuales de monitorización). Además este agente puede tener (opcionalmente) asociadas una o más direcciónes IP.

El agente puede tener asociados módulos remotos, obtenidos a través de servidores de Red, Plugin, etc.

El agente también puede tener asociados módulos de tipo "local", que son los que están definidos en la configuración del agente Software y que también se deben definir en el "Agente" de la consola WEB. Cuando un paquete de datos llega por primera vez desde el agente, si este está en modo "autoaprendizaje" (viene así por defecto), se crean estos modulos "locales" de forma automática en la consola WEB.

Por tanto, un Agente puede contener módulos de tipo remoto o de tipo local. Los módulos de tipo remoto son ejecutados por aquellos servidores que obtienen información de forma remota (incluido el prediction), y los módulos de tipo local son obtenidos por el servidor de datos (Data Server).

Agente Software

Un agente software, instalado en una máquina remota, diferente por completo a la del servidor o la consola WEB de Pandora. El agente software obtiene información "local" de la máquina donde se está ejecutando, mediante comandos que obtienen información del sistema.

Los agentes software de Pandora FMS están basados en lenguajes nativos de cada plataforma: ShellScripting para Unix que incluye GNU/Linux, Solaris, AIX, HPUX y BSD, así como IPSO de Nokia (sistema operativo de los cortafuegos Check Point).

Los agentes de Pandora FMS se pueden desarrollar prácticamente en cualquier lenguaje, siempre que cumpla la API de intercambio de datos con el servidor de datos Pandora FMS (definido por un XML de intercambio de datos). Los agentes Windows se desarrollan en un entorno libre para C++ (Mingw) y emplean la misma interfaz y modularidad que los agentes UNIX, aunque con bastantes particularidads propias.

Fichero de datos XML

El fichero de datos tiene la siguiente sintaxis:

```
<nombredehost>.<nº de serie>.data
```

Este fichero de datos es una estructura XML y su nombre se forma mediante la combinación del nombre del anfitrión o host donde está el agente, un número de serie diferente para cada paquete de datos y la extensión .data que indica que es un paquete de datos.

```
<nombredehost>.<nº de serie>.checksum
```

El fichero de datos es el fichero con extensión .data. El fichero de verificación, con extensión .checksum contiene un hash MD5 del fichero de datos. Esto permite hacer una última verificación para asegurarse de que los datos no han sido alterados de ninguna manera antes de ser procesados.

El fichero de datos XML que genera el agente es el corazón de Pandora FMS. En él se contiene un paquete de datos con la información recogida por el Agente. Este paquete de datos tiene un diseño compacto, flexible y ligero que permite que cualquier usuario pueda utilizar los agentes de Pandora FMS o sus propios desarrollos para generar información y que esta sea procesada en Pandora FMS.

El fichero de datos es un XML similar al siguiente:

```
<agent data os_name=”SunOS” os_version=”5.8” timestamp=”300”
agent_name=”pdges01”
version=”1.0”>
<module>
<name>FTP Daemon</name>
<type>generic_proc</type>
<data>0</data>
</module>
<module>
<name>DiskFree</name>
<type>generic_data</type>
<data>5200000</data>
</module>
<module>
<name>UsersConnected</name>
<type>generic_data_inc</type>
<data>119</data>
</module>
<module>
<name>LastLogin</name>
<type>generic_data_string</type>
<data>slerena</data>
</module>
</agent_data>
```

Agente físico

Pandora FMS tiene un agente físico montado sobre un router Asus. Este andén junto con los sensores conectados consigue, por el momento, monitorizar las siguientes características ambientales:

- Humedad
- Temperatura
- Luz ambiental
- Presencia

Los sensores son fácilmente calibrables al ser electrónicos, y sus valores también son fácilmente procesables por Pandora FMS.

El hecho de que el sensor sea un router con características inalámbricas abre un mundo de posibilidades a este tipo de sensores, ya presentes en algunos CPD de Empresas españolas.

6.6.14.6..Funcionamiento de Pandora FMS

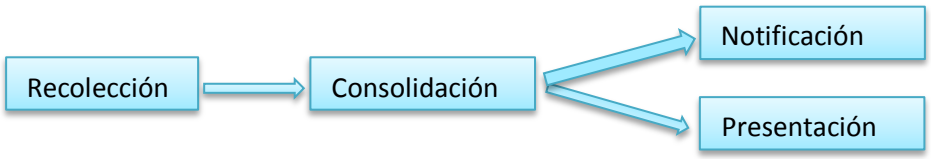


Figura 25: Funcionamiento de Pandora FMS

Autor: William Pullutaxi

Recolección

La recolección de información de todos los sucesos de los nodos que componen la red Empresarial se lo realiza mediante:

- Agentes
- Sin Agentes
- Detección Automática

Pandora FMS puede monitorizar cualquier proceso o sistema que mediante un comando devuelva un valor, así como cualquier valor dentro de un registro de texto, del sistema operativo, fichero de registro o similar. Algunos ejemplos de implementaciones ya existentes pueden ser los siguientes:

Mediante agentes Mediante agentes

- Número de conexiones (sesiones) de Checkpoint.
- Número de sesiones de NAT de Checkpoint.
- Número de conexiones de los cortafuegos para GNU/Linux NetFilter/IPTables.
- Número de paquetes registrados.
- Número de paquetes descartados.
- Número de paquetes aceptados.
- Estado de la alta disponibilidad.
- Ultima política instalada en un módulo de Firewall.
- Estado de la sincronización de los módulos.
- CPU del sistema: idle, user y system.
- Número de procesos del sistema.
- Temperatura de la CPU de un sistema.
- Valor de un registro Windows.
- Procesos en cola de un dispatcher genérico.
- Memoria del sistema: libre, swap, kernel, caché, etc.
- Porcentaje de espacio libre en disco (por diferentes particiones).
- Mensajes procesados por una puerta de enlace de correo.
- Existencia de una cadena en un archivo de texto.
- Tráfico por IP (filtrando según las conexiones de los cortafuegos).
- Visualizaciones de páginas en servidores HTTP (Apache, iPlanet, IIS, etc.).
- Porcentaje de paquetes erróneos en una puerta de enlace.
- Conexiones establecidas en un servidor de acceso remoto (RAS).
- Tamaño de un fichero concreto.
- Sesiones abiertas por un servidor VPN.
- Rendimiento MySQL: Consultas e inserciones por segundo, nivel de caché empleada, acierto de caché, consultas lentas, sesiones simultáneas,

- Estado de sistemas Snort (eventos por segundo, estado de los sensores, políticas cargadas, etc).
- Tasa de transferencia media en una herramienta de transferencia de ficheros.
- Número de peticiones DNS atendidas por un servidor (incluyendo tipos).
- Numero de sesiones FTP atendidas por un servidor FTP.
- (Genérico) Estado de cualquier proceso/servicio activo en el sistema.
- (Genérico) Estado de cualquier parámetro cuantificable del sistema.

Sin agentes (monitorización remota)

- Conocer si un sistema responde a PING (si está vivo o no).
- Conocer el tiempo de latencia de un sistema (en milisegundos).
- Saber si un puerto remoto TCP está abierto o no.
- Conocer el estado de un sistema remoto TCP en función de una respuesta a una cadena enviada.
- Por ejemplo, esto vale para saber si la versión SSH de un sistema remoto está activo y no ha cambiado.
- Esto también valdría para verificar que una página Web no ha sido alterada y que responde bien.
- Obtener información mediante SNMP.
- Saber si un puerto remoto UDP responde.
- Eventos proporcionados por IDS (Snort) hasta seis niveles de prioridad o por grupos.
- Número de conexiones locales (TCP, UDP, sockets UNIX) y estadísticas detalladas de la capa de red del S.O. (fragmentación de paquetes, pérdidas, paquetes marcianos, y otros muchos tipos de anomalías detectadas por el kernel).
- Antivirus detectados por una pasarela Web Antivirus.

- Tiempo de latencia ICMP hacia un equipo.

Consolidación

En esta instancia lo que se hace es la normalización de toda la información recolectada, Base de datos de histórico de alta capacidad para guardar datos de varios años para su uso posterior.

Notificación

Lo que se hace en esta parte es el envío de notificaciones y establecer acciones correctivas ante cualquier evento negativo que perjudique el buen funcionamiento de la red.

Presentación

Este software permite mostrar los datos obtenidos de toda la red en:

- INFORMES
    - Tendencias
    - Inventario
    - Top– N
    - SLA
    - Gráficas
    - Envío programado en PDF
- CUADROS DE MANDO
- MAPAS VISUALES
- ÁRBOLES DE SERVICIO
- MAPAS TOPOLÓGICOS
- VISTAS DE ÁRBOL

6.6.15. Implantación del Sistema.

6.6.15.1.Requerimientos

Para la implementación del sistema la Institución cuenta con una infraestructura de red de comunicaciones para ofrecer una solución diseñada a medida de las

necesidades operativas de las actividades de negocio. Adicionalmente, los servidores y las bases de datos, deben tener mecanismos de protección que garanticen su disponibilidad, integridad y confidencial.

Las medidas que se pueden considerar deben conjuntar una solución que se implementa a nivel de red y a nivel host. Ambas deben complementarse con el desarrollo de una cultura informática de buenas prácticas y de Políticas de Seguridad.

En primera instancia, es necesario distinguir la procedencia del tráfico que entra y sale de la red local, conocer su origen y destino para asignarles propiedades de paso; y al mismo tiempo garantizar que los paquetes "no van" a sitios restringidos.

Los servidores, deben clasificarse en públicos y privados para ponerlas en redes distintas con niveles de acceso distintos y mecanismos de protección distintos.

Cada uno de los miembros de la Empresa, cumplen funciones distintas, por lo que todos tienen el mismo nivel de acceso a la información o a los servicios asociados. Tampoco la prioridad de acceso es la misma, por lo que es fundamental asignar perfiles de acceso a nivel de red, servicios y datos.

Es imperativo, la implementación de mecanismos de control que permitan filtrar el tráfico. Detectar paquetes no deseados y solucionar problemas de seguridad.

6.6.15.2.Análisis de las características actuales de la red Empresarial

Después de haber revisado la instalación y basándonos en los siguientes puntos:

- Topología de red
- Ubicación de servidores y puntos de acceso
- Análisis de los dispositivos con el fin de identificar aspectos de hardware y software que puedan influir en la implementación.

Procederemos a realizar la descripción de la situación actual sobre los equipos, instalación de red y las seguridades con la que cuenta la Empresa.

En la siguiente figura se muestra como está estructurado cada uno de los equipos de la Empresa, mismas que a continuación se detallara cada una de las características.

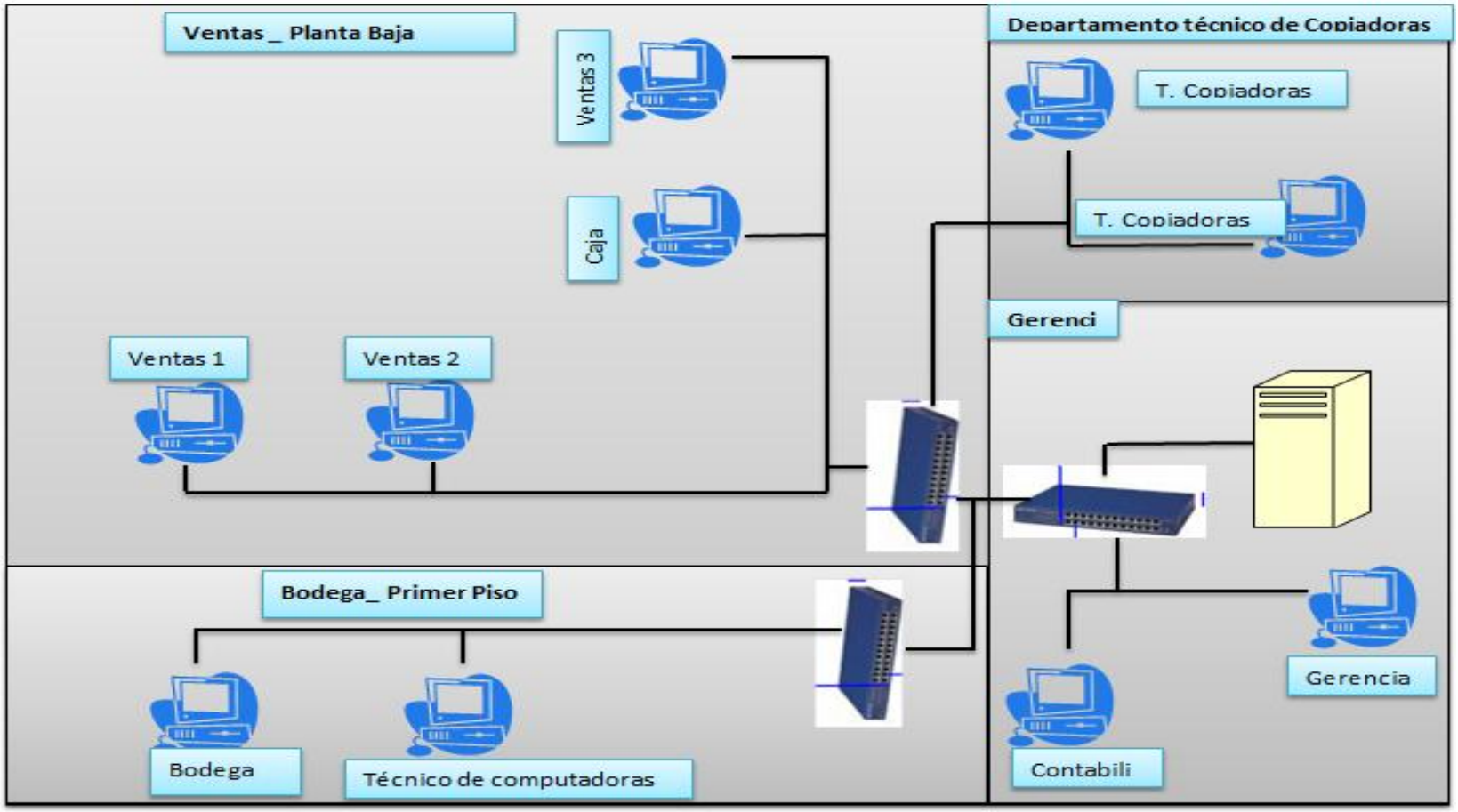


Figura 26: Diagrama de distribución de la red de la Empresa Importadora REPCOPY

Autor: William Pullutaxi

Se tiene que realizar un estudio que determine que aplicaciones y que protocolos se están empleando, así como las necesidades de ancho de banda que se requieren. La siguiente tabla resume estos aspectos.

DEPARTAMENTO	TIPO DE RED	NÚMERO DE USUARIOS	NÚMERO DE DISPOSITIVOS
GERENCIA	Alámbrico	1	2
Dpto. Técnico	Alámbrico	2	2
Ventas	Alámbrico	4	3
Contabilidad	Alámbrico	2	2
Caja	Alámbrico	1	1
Bodega	Alámbrico	1	2

Tabla 22: Resumen de la Auditoria de la red Empresarial

Autor: William Pullutaxi

Ya con una vista general de cómo está la estructura de la Empresa y en los departamentos en los que se dividen, procederemos a revisar cada una de las características de los equipos que están actualmente instalados en la Institución.

Arquitectura y configuración de Hardware y Software

- **Equipos de computo**
  - **Perfiles de las estaciones de trabajo**

    El perfil de los equipos informáticos con los que cuentan la Empresa en lo que respecta a estaciones de trabajo es la siguiente:

CARACTERÍSTICAS	ESCRITORIO	PORTÁTILES
Cantidad	10	1
Marca	Intel	Hp
Velocidad	2.8 GHZ	1.08 GHZ
Microprocesador	Dual core	Dual core

Memoria RAM	2 GB	2 GB
Capacidad de Almacenamiento	500 GB	750 GB

Tabla 23: Perfiles de estaciones de trabajos

Autor: William Pullutaxi

- **Perfil del Servidor**

El perfil básico del equipo con el que cuenta la empresa Importadora REPCOPY en lo que respecta a servidor es el siguiente.

CARACTERÍSTICA	SERVIDOR
Cantidad	1
Marca	Intel
Velocidad	2.53 GHZ
Microprocesador	Intel I7
Memoria	4 GB
Cap. de Almacenamiento	4 discos de 1.5 TB total 6 TB

Tabla 24: Perfil de Servidor Institucional

Auto: William Pullutaxi

- **Plataforma de los terminales**

En la Empresa Importadora REPCOPY, se utiliza como plataforma de trabajo **WINDOWS XP,** tanto en los equipos informáticos de escritorios como en las maquinas portátiles.

- **Plataformas de los servidores**

En la Institución, se utiliza como plataforma de trabajo para los servidores **WINDOWS SERVER 2003,** mismo que está configurado como servidor DHCP, Servidor Web

- **Sistemas Informáticos**
    - **Aplicaciones**

      Las principales aplicaciones utilizadas en la Empresa son las siguientes:

        - Internet Explorer
        - Messenger
        - Microsoft office 2010
        - Winrar
        - Avira
    - **Sistemas propios de la empresa**

      La Empresa cuenta con un sistema de inventario y facturación instalada y configura adecuadamente para el trabajo diario, llamado Microplus SQL.

- **Arquitectura y configuración de la red**

Los dispositivos mencionados a continuación están ubicados en la Empresa para tener un control del funcionamiento de la red y la seguridad de la misma.

En los diferentes departamentos de la empresa existen una serie de computadoras con las cuales se genera la red interna, incluyendo equipos de comunicación como Routers, Switch, Modem y otros.

El cable de red de los computadores se conecta mediante canaleta, dicho cable se conecta al switch, estos switch se conectan hacia un Router, mismo que está configurado de acuerdo a la empresa proveedora de internet, este Reuter a su vez se encuentra conectado hacia el modem de Internet de la Campania CTN.

Los componentes que se utilizan para el cableado estructurado en las secciones de Gerencia, Caja, Ventas, Contabilidad, Bodegas y Servicio Técnico son los siguientes:

- Cable UTP
- Conectores RJ-45

- Canaletas
- Tarjetas de Red
- Tomas de red

Una vez obtenida la información respectiva a continuación se muestra un cuadro de la configuración del servidor, las estaciones de trabajo Servidor de Internet.

DEPARTAMENTO	EQUIPO	TARJETA DE RED	IP	MASCARA	PERTA DE ENLACE
Gerencia	Servidor	Fast Ethernet NIC	192.168.1.9	255.255.255.0	192.168.1.1
Gerencia	Portátil	Fast Ethernet NIC	192.168.1.2	255.255.255.0	192.168.1.1
Caja	Computadora de escritorio	Fast Ethernet NIC	192.168.1.3	255.255.255.0	192.168.1.1
Ventas 1	Computadora de escritorio	Fast Ethernet NIC	192.168.1.4	255.255.255.0	192.168.1.1
Ventas 2	Computadora de escritorio	Fast Ethernet NIC	192.168.1.5	255.255.255.0	192.168.1.1
Ventas 3	Computadora de escritorio	Fast Ethernet NIC	192.168.1.6	255.255.255.0	192.168.1.1
Contabilidad	Computadora de escritorio	Fast Ethernet NIC	192.168.1.7	255.255.255.0	192.168.1.1
Bodega 1	Computadora de escritorio	Fast Ethernet NIC	192.168.1.7	255.255.255.0	192.168.1.1
Bodega 2	Computadora de escritorio	Fast Ethernet NIC	192.168.1.8	255.255.255.0	192.168.1.1
Servicio Técnico	Computadora de Escritorio	Fast Ethernet NIC	192.168.1.9	255.255.255.0	192.168.1.1

Tabla 25: Diagrama físico de la red

Autor: William Pullutaxi

A más de la red cableada cuenta con la red inalámbrica para la conexión de los equipos portátiles que son cargadas de programas para la venta.

A continuación veremos un cuadro con las características de los equipos de conexión de las estaciones de trabajo utilizadas para su interconexión.

Equipo	Modelo	N de puertos
Modem		4
Router	D Link	8
Switch (4)	D Link	8

Tabla 26: Equipos de conexión entre los equipos

Autor: William Pullutaxi

- **Seguridad**

Todas las computadoras de los departamentos y secciones tienen instalado un antivirus llamado Avira quien monitorea a cada estación de trabajo de manera independiente y actualiza automáticamente.

Además cada uno de los responsables de las computadoras tienen su usuario y contraseña, para mayor seguridad de la información ya que en su mayoría los equipos no tienen el control de acceso y se pueden modificar o perder información.

En lo que respecta a monitoreo de las amenazas de los ciber delincuentes no cuentan con una política o herramientas que ayude a minimizar la vulnerabilidad de las redes, tampoco cuentan con un plan de contingencia ante un ataque que pueda sufrir la Institución.

- **Gestión y Administración**

La administración de los usuarios de la red se encarga un responsable de la sección de Procesamiento de Datos que es el Gerente, esta persona es quien

elabora roles, permisos, creación de usuarios, contraseñas para las computadoras de los departamentos de la Empresa.

También es el encargado de revisar que todos los equipos de red estén funcionando en su totalidad para entregar un mejor servicio a los clientes de la Empresa.

- **Manejo de respaldos**

Para respaldar la información resultante de cada uno de los procesos que se realizan en las diferentes áreas de trabajo dentro de la Institución, el gerente lleva a cabo los siguientes procesos:

  - Los respaldos o backups de la información son realizados de forma automática diariamente al concluir el horario de trabajo de cada una de las áreas, dichos respaldos son realizados en el mismo servidor.
  - La información que se respalda es la resultante de los procesos de la recaudación y cobros de las ventas del día, así como también ingreso y egreso de mercadería.
  - Cabe destacar que la información respaldada reposa en un único servidor, pudiendo este ser víctima de daño o fallas, misma que provocaría perdida de todas las transacciones realizadas en la institución, provocando grandes pérdidas económicas y tiempo.

- **Planes de contingencia**

En la actualidad, en la Empresa Importadora REPCOPY no cuenta con un plan de contingencia que ayude a salvaguardar la integridad de los recursos informáticos ya sea estos equipos o información.

Una vez realizada la auditoria de la red, se determina lo que se puede aprovechar de la instalación de la LAN para analizar y definir una estrategia de mejoramiento de la misma.

Primeramente se determina los requerimientos del negocio y se especifican los aspectos claves como el grado de disponibilidad de red o las características de la operación continua. Un punto importante es el análisis del impacto que supondría la pérdida del servicio, tanto en cuanto a pérdidas de beneficios como la pérdida de mercado.

El resultado son los objetivos del nivel de servicio que deben quedar recogidos y registrados adecuadamente.

Densidad de usuario

Uno de los datos que es importante conocer a la hora de dimensionar cualquier tipo de red es determinar el número de usuarios simultáneos que deberá soportar el sistema. Resulta conveniente tener en cuenta la previsiones de crecimiento de personal en la Empresa, en nuestro caso no es muy grande la cantidad de usuarios, aunque en el futuro se piensa ampliar.

De tal forma que hemos obtenido la siguiente tabla donde se indica el número de empleados.

NIVEL	DEPARTAMENTO	NÚMERO DE EMPLEADOS
Planta baja	Ventas	5
	Gerencia	1
	Técnico de Copiadoras	5
	Contabilidad	2
	Caja y cobranzas	1
Primer piso	Bodega	1
	Técnico de computadoras	1

Tabla 27: Tabla de distribución de departamentos y empleados

Autor: William Pullutaxi

Después de haber evaluado los requerimientos y establecido la cantidad de usuarios a los que se va a beneficiar, se determinó que el diseño de la red, que incorpora la Empresa actualmente se muestra en la figura 27 pág. 94.

6.6.16. Instalación de Pandora FMS

Una vez estudiado los dispositivos, la estructura de la red, a continuación pasaremos a la instalación del sistema Pandora FMS:

Para la instigación de Pandora FMS es necesario cumplir con algunos requisitos necesarios para el buen funcionamiento del mismo.

6.6.16.1..Cuestiones previas a la instalación

Es recomendable seguir el siguiente orden al instalar Pandora FMS:

- Instalar la consola
- Instalar el servidor
- Verificar el funcionamiento

La razón es que la base de datos MySQL que usa el servidor se crea en el proceso de configuración inicial de la consola, y por ello para asegurar el correcto funcionamiento del servidor es recomendable realizar primero el proceso de instalación completo de la consola.

Además no es necesario que la consola y el servidor de Pandora FMS se encuentren alojados en la misma máquina, ya que es posible indicarle al servidor dónde se encuentra la base de datos MySQL mediante el archivo de configuración del servidor.

La instalación del agente la podemos realizar sin ningún problema antes o después de instalar el servidor y la consola ya que es independiente de estos y puede estar instalado en cualquier máquina.

En este apartado se ha tratado únicamente los requisitos previos a la respectiva instalación de nuestro servidor de Pandora FMS, los pasos de instalación y configuración están detallados en el apartado de anexos.

6.6.16.2..Operación de Servidor de Pandora FMS

Toda la interacción del usuario con Pandora FMS se realiza a través de la consola WEB. La consola de Pandora FMS es una consola WEB que sigue los últimos estándares y tecnologías WEB, por lo que requiere un navegador avanzado y el uso opcional de Flash. Se recomienda Firefox 2.x o superior. También puede usarse Internet Explorer 8, aunque este provee una experiencia de usuario más incómoda por su manera particular de gestionar algunos controles WEB.

Agentes en Pandora FMS

Toda la monitorización que realiza Pandora FMS se organiza a través de una entidad genérica llamada "agente", que está dentro de un bloque más genérico, llamado grupo. Un agente sólo puede pertenecer a un grupo.

La información se ordena de forma lógica mediante una jerarquía basada en grupos, agentes, grupos de módulos y módulos. Existen agentes basados únicamente en la información proporcionada por un agente software e instalados en el Sistema, y agentes con información exclusiva de red, información que no procede de un agente software, donde no hay necesidad de instalar ningún software, y que ejecuta las tareas de monitorización de red desde los servidores de red de Pandora FMS.

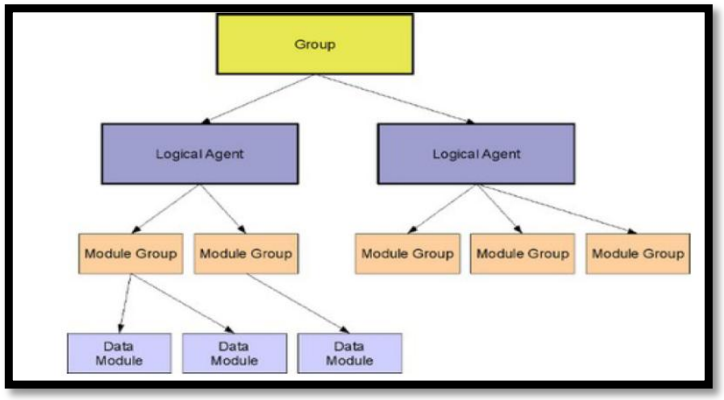


Figura 27: Esquema organizativo de un agente

Fuente: http://pandoraFMS.com/pandora/doc/es

De igual manera, existen agentes que tienen tanto información de red, como información obtenida mediante agentes software.

La información se recoge en módulos que están asignados (de forma lógica) a agentes de Pandora FMS en la consola. Es importante distinguir el concepto de agente (de donde cuelgan los módulos, que contienen la información recolectada) de los agentes software que se ejecutan en sistemas remotos.

- **Monitorización con agente software**

Los datos recogidos por los agentes software se almacenan en pequeñas piezas de información llamadas «módulos». Cada módulo almacena sólo un tipo de dato. El valor de cada módulo es el valor de una variable supervisada. Una vez que el agente comience a enviar la información, los datos empezarán a consolidarse en la base de datos y se podrá tener acceso a los mismos.

Los agentes software de Pandora FMS utilizan los comandos propios del sistema operativo para obtener la información. El servidor de datos de Pandora FMS almacena y procesa los datos generados por estos comandos y transmitidos al servidor dentro de un fichero XML. La información devuelta por esos comandos está contenida en lo que llamamos «Módulos».

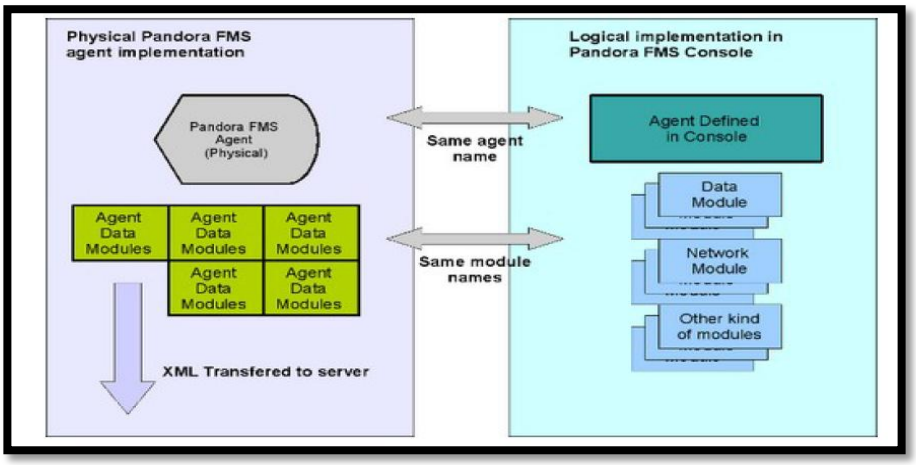


Figura 28: Esquema del agente software

Fuente: http://pandoraFMS.com/pandora/doc/es

Cuando el agente software se ejecuta por primera vez, envía un XML al servidor de datos de Pandora FMS, que lo recibe a través de tentacle, SSH o FTP en el directorio de entrada del servidor.

El servidor de datos revisa ese directorio cada cierto tiempo y cuando encuentra un fichero, lo procesa. Al abrir ese fichero de datos, consistente en un XML, identifica el agente por su nombre, de forma única, es decir, cada agente tiene que tener un nombre completamente único, donde las mayúsculas y las minúsculas son diferenciadas por Pandora FMS. El servidor, por defecto, crea automáticamente todos los agentes de los cuales recibe datos y no están dados de alta en la BBDD.

De la misma manera, si el agente se ha añadido en modo «aprendizaje», los módulos enviados que no estén definidos previamente en el agente, serán creados por el servidor automáticamente.

Antes de pasar a presentar datos de monitoreo y la presentación de resultados de la implantación del sistema de monitoreo procederemos a explicar los parámetros en que se basaran los resultados de monitoreo de los sucesos producidos durante la monitorización de los diferentes servicios.

- Color naranja Estado de Alertas disparadas
- Color rojo Estado Crítico
- Color amarillo Estado de Advertencia
- Color gris Estado Desconocido
- Color verde Estado Normal

Para la monitorización de la red debe estar instalado correctamente el servidor de Pandora así como los diferentes servicios.

Otro de los siguientes pasos es haber creado los agentes, estos agentes serán considerados como las estaciones de trabajos (computadoras terminales)

Una vez creado los agentes debemos asignarles módulos a nuestros agentes con sus respectivas alertas.

La información de la creación de agentes, módulos, alertas, etc. se detallara en los apartados anexos creación de agentes, módulos, alertas.

6.6.17. Presentación de resultados

En este punto del proyecto se tratara de los resultados que se pueden obtener con este sistema después de ser víctimas de un ataque que sufre la red.

A. Ataque

Como ya se explicó anterior la herramienta utilizada para realizar el ataque es bactrack 5 y el ataque en si es mediante metasploint.

Cuando iniciamos nuestro live cd de bactrack 5 nos aparece instalado en modo texto, para poder ingresar nos pide el Login y la contraseña,

El Login es: root

La contraseña: toor

Hasta este punto estamos en modo texto, lo que debemos hacer es digitar el comando **startx** para que cambiemos a modo gráfico.

Comenzamos obteniendo nuestra ip local para saber dónde estamos ubicados en la red. Para ello ya dentro de BackTrack **Abrimos una Terminal** (Ctrl+Alt+T) y escribimos: **ifconfig**

Figura 29: Exploración de la ip de la maquina atacante

Autor: William Pullutaxi

Como podemos ver **nuestra IP local es 192.168.0.115**, otro tipo. **Apuntamos esta dirección** porque nos servirá más adelante.

Escaneamos la red con **nmap** para obtener la dirección IP de los posibles objetivos. Como nuestra IP local es 192.168.0.115, buscaremos objetivos entre el rango 192.168.0.100 y 192.168.0.130, para ello escribimos lo siguiente

Nmap –v –sS –O 192.168.0.100-130

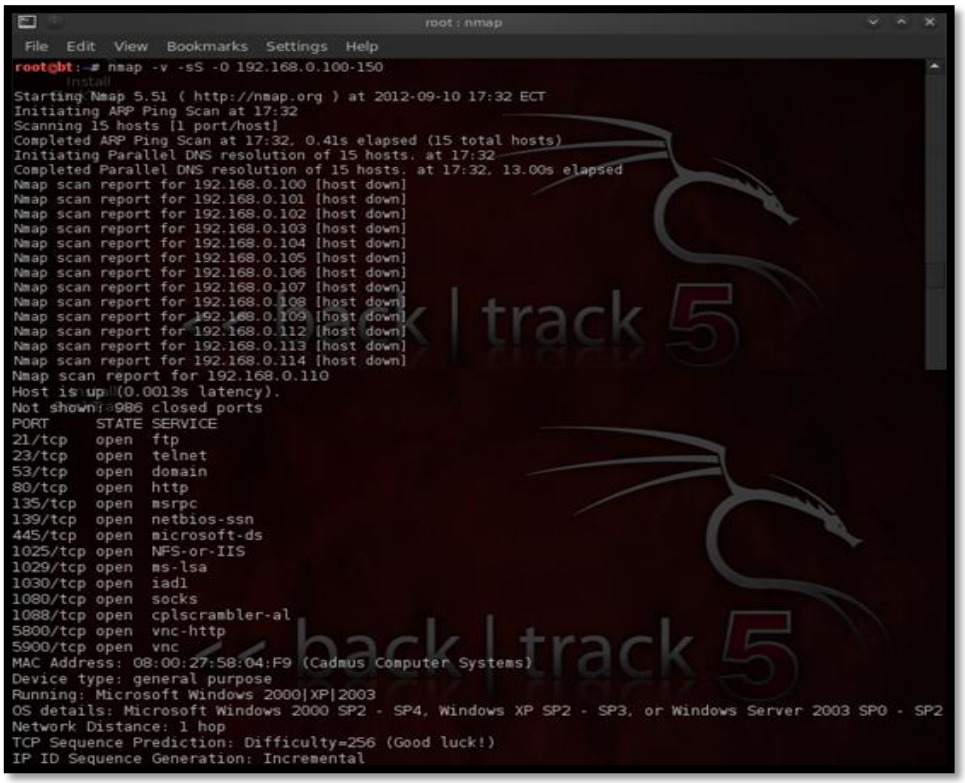


Figura 30: Escaneo de las ip de toda la red

Autor: William Pullutaxi

Como podemos ver tenemos una PC con Windows XP, 2000 o 2003 que **posiblemente es vulnerable al ataque**. Y su IP es **192.168.0.110**. **Apuntaremos esta IP** para usarla después como se puede apreciar en la imagen nos muestra también los puertos que están abiertos por los cuales podemos realizar los ataques.

Si ya tenemos la IP del objetivo no es necesario hacer este paso así que simplemente lo saltean.

Ya sabemos nuestra IP y la IP del objetivo así que ahora procederemos al ataque. **Abrimos Metasploit** escribiendo en la terminal:

msfconsole

Nos saldrá algo así:

Figura 31: Abriendo el metaexplit

Autor: William Pullutaxi

Seleccionaremos el exploit que utilizaremos para realizar el ataque a la víctima.

Para esto nos dirigimos a la siguiente dirección /pentest/exploits/framework2 y ejecutamos el exploits con ./msfconsole

Figura 32: Ingresando al exploit

Autor: William Pullutaxi

Para poder mostrar los exploits debemos digitar el comando **show exploit**

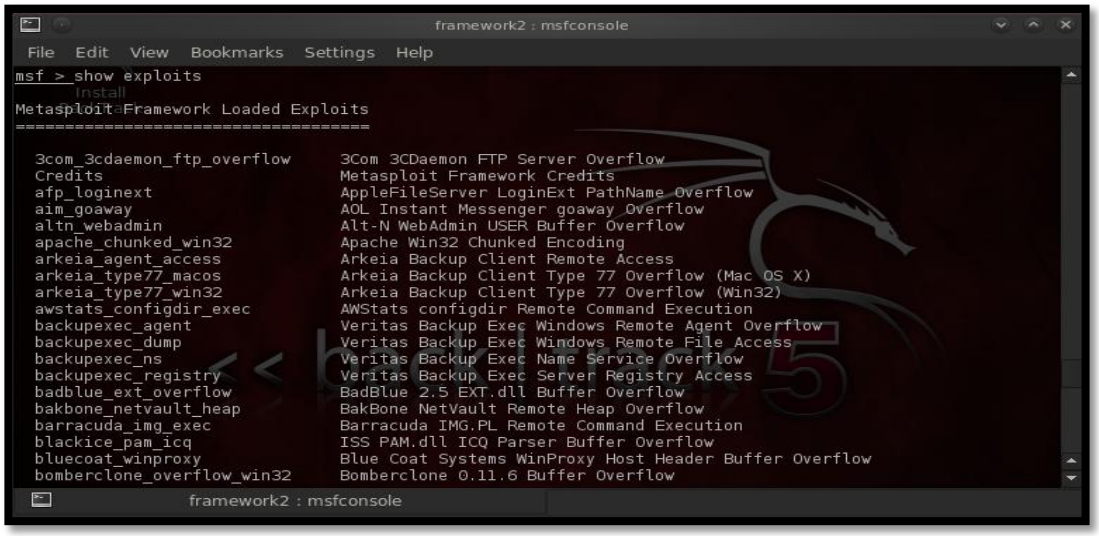


Figura 33: Vista de los exploit disponibles para el ataque

Autor: William Pullutaxi

Como podemos ver tenemos en la pantalla los exploits que podemos utilizar para realizar el ataque.

El siguiente paso es elegir el exploit que utilizaremos para atacar a la víctima, en este caso elegimos el exploit Windows/smb/ms08_067_netapi

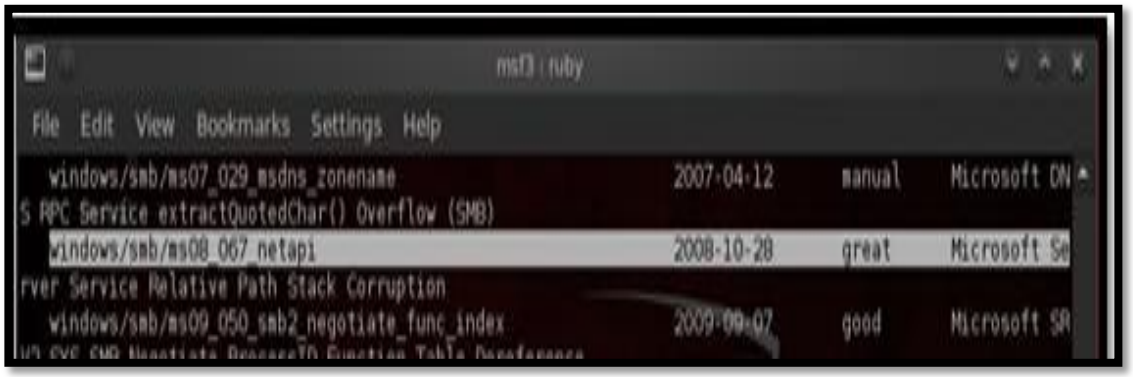


Figura 34: Selección del exploit a utilizar

Autor: William Pullutaxi

El siguiente paso es usar el exploit para eso ejecutamos:

Use Windows/smb/ms08_067_netapi

Ahora debemos ver los payloads que son compatibles con el exploit seleccionado digitamos **show payloads.**

Figura 35: Vista de los payloas a utilizar en el ataque.

Autor: William Pullutaxi

Ejecutamos el payload con el comando **set payload Windows/Shell_bind_tcp** que nos abrirá una Shell.

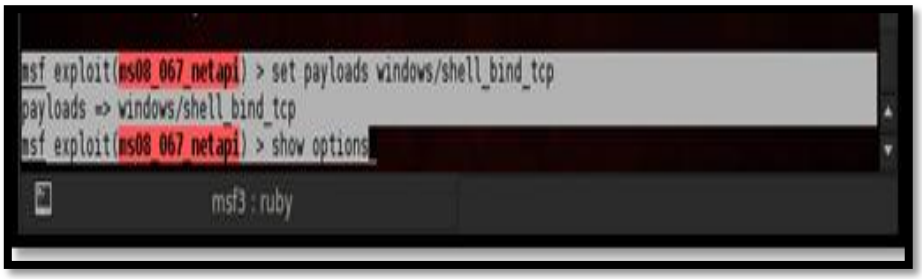


Figura 36: Ejecución del payload seleccionado

Autor: William Pullutaxi

Ejecutamos **show options** para ver los parámetros necesarios antes de ejecutar el ataque.

Figura 37: Vista de los parámetros disponibles para el ataque.

Autor: William Pullutaxi

Como podemos ver ahora solo nos falta el RHOST que corresponde a la ip de la víctima, añadimos la ip de la víctima con el comando set RHOST 192.168.0.110 y para comprobar la ip de RHOST ejecutamos **show options**

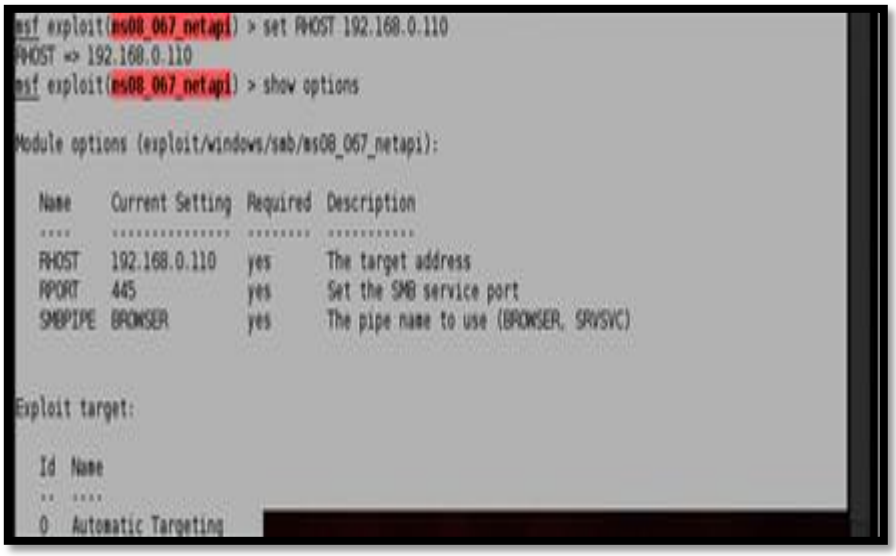


Figura 38: Agregando IP victima a RHOST

Autor: William Pullutaxi

Ejecutamos el ataque con el comando **exploit**

Figura 39: Ingreso al servidor víctima.

Autor: William Pullutaxi

Como podemos observar hemos conseguido ingresar a la shell de nuestra víctima de ahora en adelante podemos hacer y deshacer lo que nosotros queramos. En este caso vamos a detener el servicio DHCP, que influye mucho en el trabajo diario de la Empresa.

Figura 40: Vista del funcionamiento de los servicios en la víctima en Pandora FMS

Autor: William Pullutaxi

En la figura anterior podemos observar que el servicio DHCP está funcionando correctamente. Al igual que su alerta está en estado funcionando correctamente. Para esto debemos tener conocimiento de los comandos de Windows para poder realizar operaciones dentro de la maquina víctima.

El comando que utilizaremos es **net stop nombre de servicio**

En este caso quedaría así**: net stop DHCPServer** y nos aparece un mensaje que confirma la acción realizada sobre la víctima.

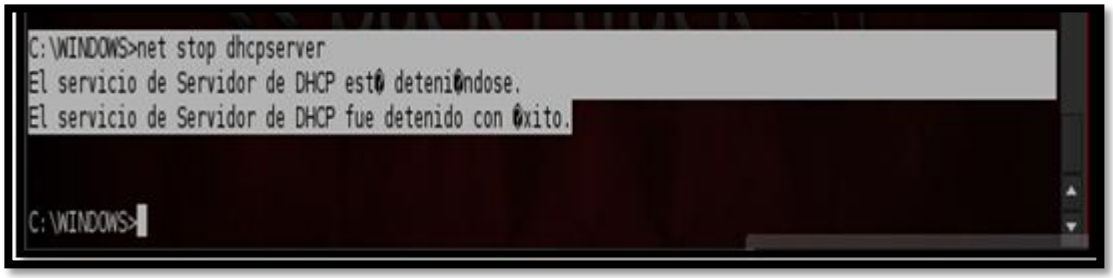


Figura 41: Ejecución del ataque.

Autor: William Pullutaxi

El último paso es verificar que nuestro sistema pandora devuelva la alerta correspondiente a este servicio, en el grafico anterior se puede observar como el control del servicio DHCP está en estado funcionando correctamente, una vez realizado el paso anterior el estado debe cambiarse a color rojo que sería estado crítico.

Figura 42: Comprobación del ataque en PANDORA FMS

Autor: William Pullutaxi

Como podemos apreciar en la imagen anterior el estado del módulo de chequeo del servicio DHCP cambio a color rojo es decir que nos indica que ha pasado algo con el servicio DHCP y también el estado de la alerta se cambia y se dispara enviando un mail al correo electrónico establecido.

Este es uno de tantos ataques se puede realizar a los servicios de la red, y como podemos darnos cuenta que tan vulnerable puede ser un servidor cuando no está correctamente protegido.

B. Monitorización vista clásica

Nos muestra información general de todos los agentes, los módulos asignados a los agentes, las alertas que en estas existen y las acciones realizadas por el usuario sobre los agentes.

Figura 43: Vista clásica de los agentes

Autor: William Pullutaxi

C. Vista de grupo

Esta vista nos presenta información de los agentes en grupos es decir nos muestra, información aislada de los servidores, información del servidor de pandora y el servidor de la Empresa.

Figura 44: Presentación de datos en vista en grupo de agentes.

Autor: William Pullutaxi

En el grafico podemos observar la información obtenida de los agentes, en nuestro caso tenemos 10 agentes es decir 10 máquinas trabajando en la red, 7 agentes desconocidos es decir en la toma de la imagen hay 7 máquinas que no estas prendidas, 55 módulos que no están levantados en las 7 máquinas que no estas prendidas, vemos que no hay ningún agente que eta sin iniciar una sola vez, 24 que están funcionando normalmente, 5 módulos o funciones que están en estado crítico, y una alerta enviada por el agente.

D. Vista de árbol

Muestra la misma información de la vista anterior pero en forma de árbol.

Figura 45: Información de los agentes en vista de árbol.

Autor: William Pullutaxi

E. Vista de agentes

Esta vista nos presenta en primera instancia todos los agentes que existen en nuestra red.

Figura 46: Vista de agentes
Autor: William Pullutaxi

La imagen nos muestra los 10 agentes que existen en nuestra red en que grupo esta creado, en este caso creado en Repcopy el tipo de sistema operativo cargado en el agente, en que intervalo de tiempo se va actualizar, el estado en el que se encuentra el agente, y el tiempo de la última acción sobre el agente.

F. Información detallada de los agentes y sus módulos

Al pasar el mouse sobre el nombre del agente nos permite ver información más detallada de los agentes, es decir los módulos que contienen los agentes, alertas asignadas, también permite ver los datos del agente y modificar el agente

Figura 47: Vista detallada de los módulos del agente Servidor

Autor: William Pullutaxi

Como podemos observar en las imágenes anteriores los diferentes módulos creados para los agentes y en el cuadro de estado tenemos los diferentes colores con los estados de cada módulo.

En la primera imagen anterior en la parte superior derecha podemos observar un menú, misma que nos permite obtener información del agente (Maquina) y también permiten hacer diferentes operaciones en las mismas.

G. Presentación de datos

Para poder realizar la presentación de los datos procedemos a seleccionar el icono en forma de foco, mismo que al dar clic sobre este nos mostrara información de los módulos como se muestra en la figura siguiente, misma que podemos ver información diaria, por semana o por mes.

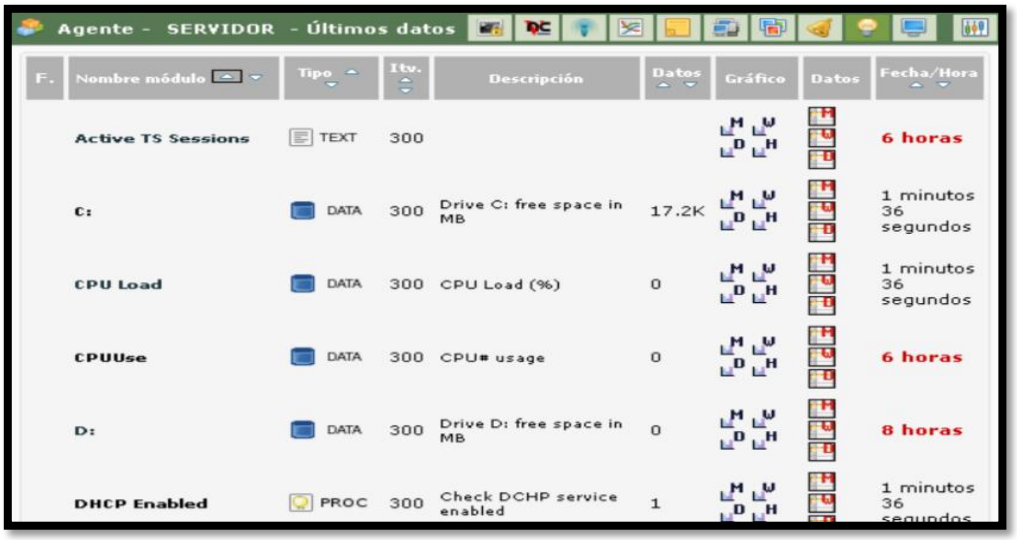


Figura 48: Presentación de datos en forma periódica

Autor: William Pullutaxi

H. Vista de alertas establecidas en cada agente

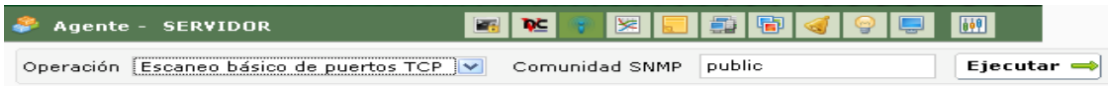
Para poder ver las diferentes alertas para cada servicio del agente se debe dar clic en el icono en forma de campana, misma que presentara la siguiente pantalla.

Figura 49: Vista de alertas en el agente servidor.

Autor: William Pullutaxi

I. Escaneo básico de puertos

Otra de las funciones que nos permite hacer pandora es el escaneo de los puertos del servidor, para esto debemos seleccionar el icono en forma de red inalambrica, una vez seleccionado este icono nos aparece la siguiente pantalla.



Debemos dar clic en ejecutar y nos muestra la pantalla con el escaneo de todos los puertos.

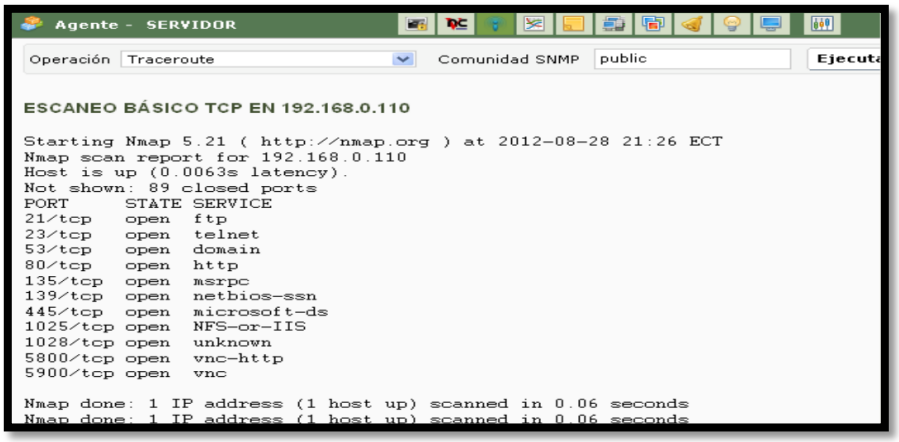


Figura 50: Escaneo de puertos del servidor

Autor: William Pullutaxi

J. Escritorio remoto

Otra de las funcionalidades que presenta pandora es la visualización en escritorio remoto del agente que deseemos sin olvidar que un agente es una maquina en la red, para esto debemos instalar un servidor vnc en la maquina a explorar, esta función ayudara a tener controlado a los empleados puesto no tienen restringidos las páginas de Internet, es decir que tienen acceso a todas las páginas del Internet, cabe destacar que esto no restringe las páginas a las que no deben acceder los empleados, de la forma que ayudara es que funciona vía Internet y el gerente en este caso podrá ver que está realizando el empleado en un determinado tiempo. Esta función tendrá solamente el Gerente de la Empresa REPCOPY puesto que no cuenta con una persona de sistemas, Para esto debemos seleccionar el icono que nos indica VNC, mismo que al dar clic presentara la siguiente pantalla.

Figura 51: Pantalla de conexión a escritorio remoto

Autor: William Pullutaxi

Como podemos observar en la figura anterior nos aparece la ip de la maquina a la que queremos ver, lo único que hay que hacer es dar clic en OK, y después nos pedirá la contraseña que debíamos haber configurado en la máquina, finalmente nos mostrara el escritorio de la máquina que accedimos.

K. Detalles de alertas

Aquí nos permite ver todas las alertas configuradas en los agentes

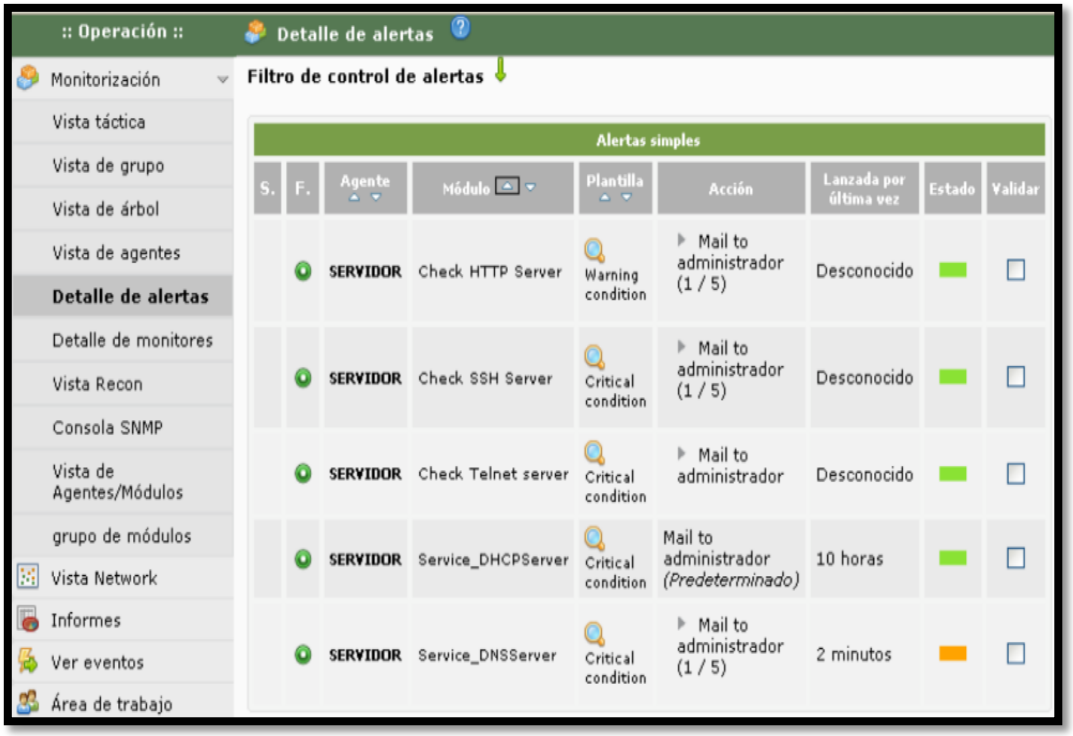


Figura 52: Filtro de control de alertas

Autor: William Pullutaxi

Para este caso se tomaron los ejemplos de las alertas establecidas en el agente servidor (servidor Empresarial).

L. Detalle de monitores

En este apartado nos permite ver los datos que se han realizado en los agentes el estado de cada agente, la hora en la que se produjo los datos.

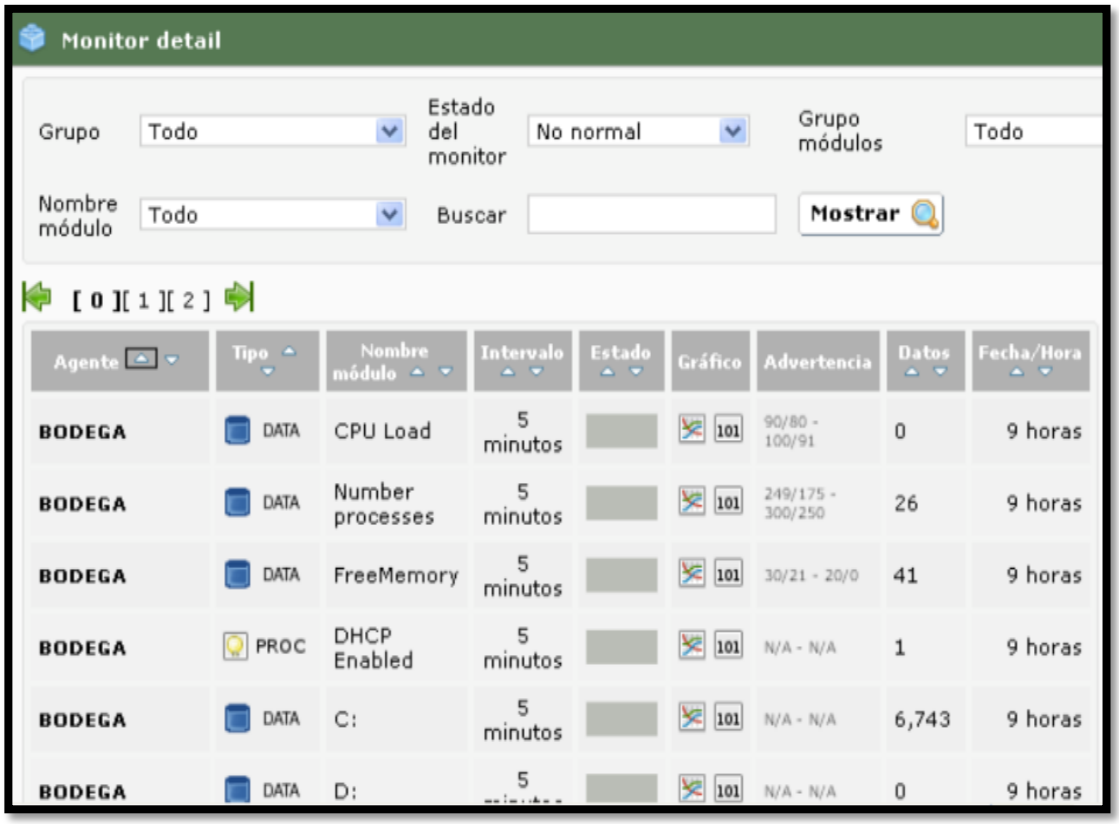


Figura 53: Detalles de monitorio de los agentes

Autor: William Pullutaxi

En esta parte del proyecto se ha explicado sobre la monitorización de los agentes con las diferentes presentaciones a la hora de presentar los datos así como los módulos que están configurados en la misma y sus respectivas alertas.

M. Vista de la red

Una de las opciones que nos da Pandora FMS es poder visualizar la red de forma gráfica como sería la red real de la Empresa.

Como podemos apreciar en figura 56 (pág. 119) anterior todas las estaciones de trabajo al igual que el servidor de datos está conectado al servidor de pandora FMS en donde se almacena toda la información de los agentes los módulos asignados a los agentes y las alertas.

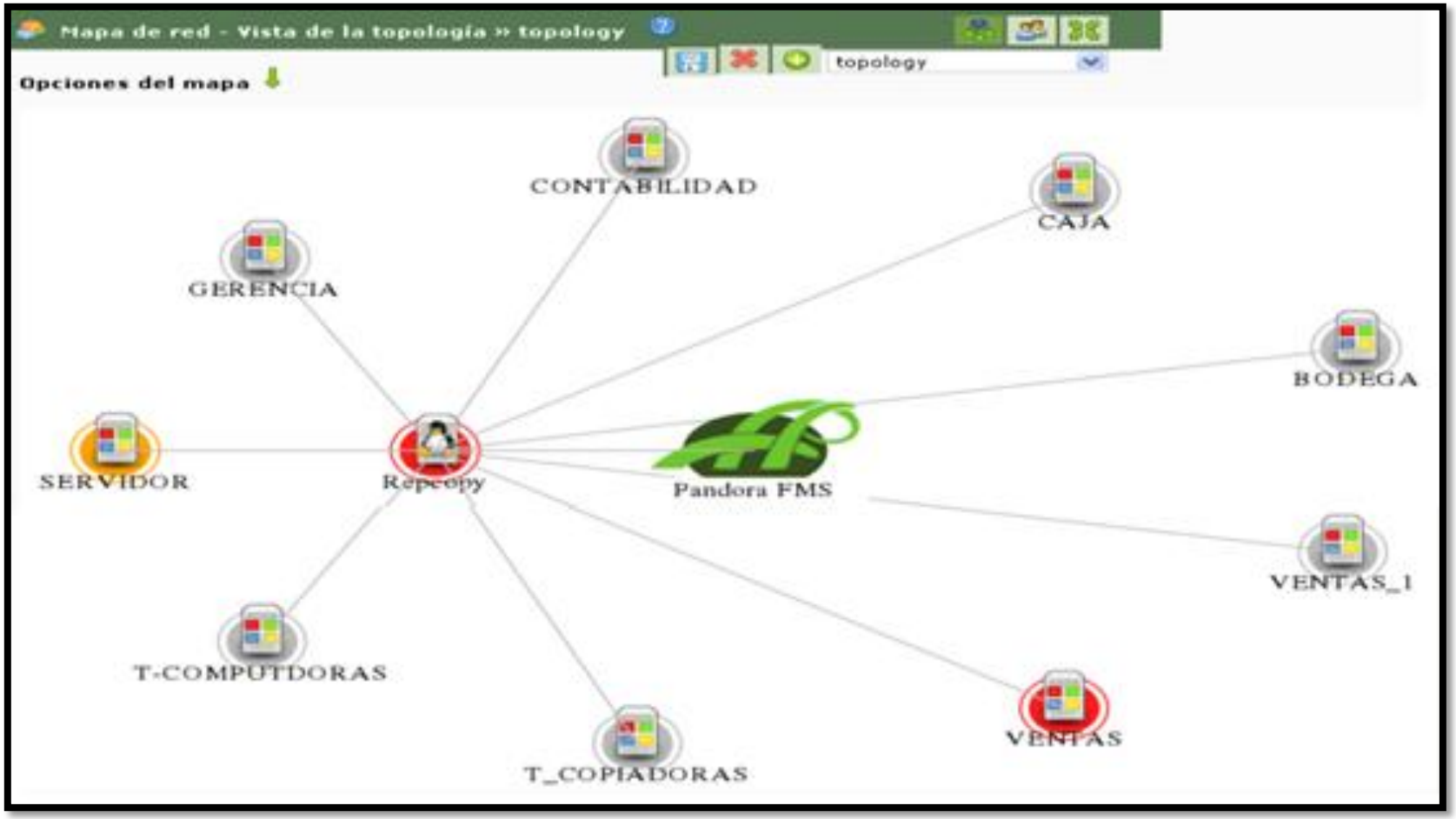


Figura 54: Vista de los agentes en forma de topología.

Autor: William Pullutaxi

N. Informes

Con Pandora FMS es posible crear informes personalizados con información de los agentes, relativa a ellos como cálculos derivados de ellos o incluso importar datos o tablas de 3º sitios con tipo Url import. Se puede seleccionar igual que con las gráficas de usuario diferentes módulos de diferentes agentes. Los datos se visualizan de diferentes formas en función del tipo de elemento de informe que deseamos añadir.

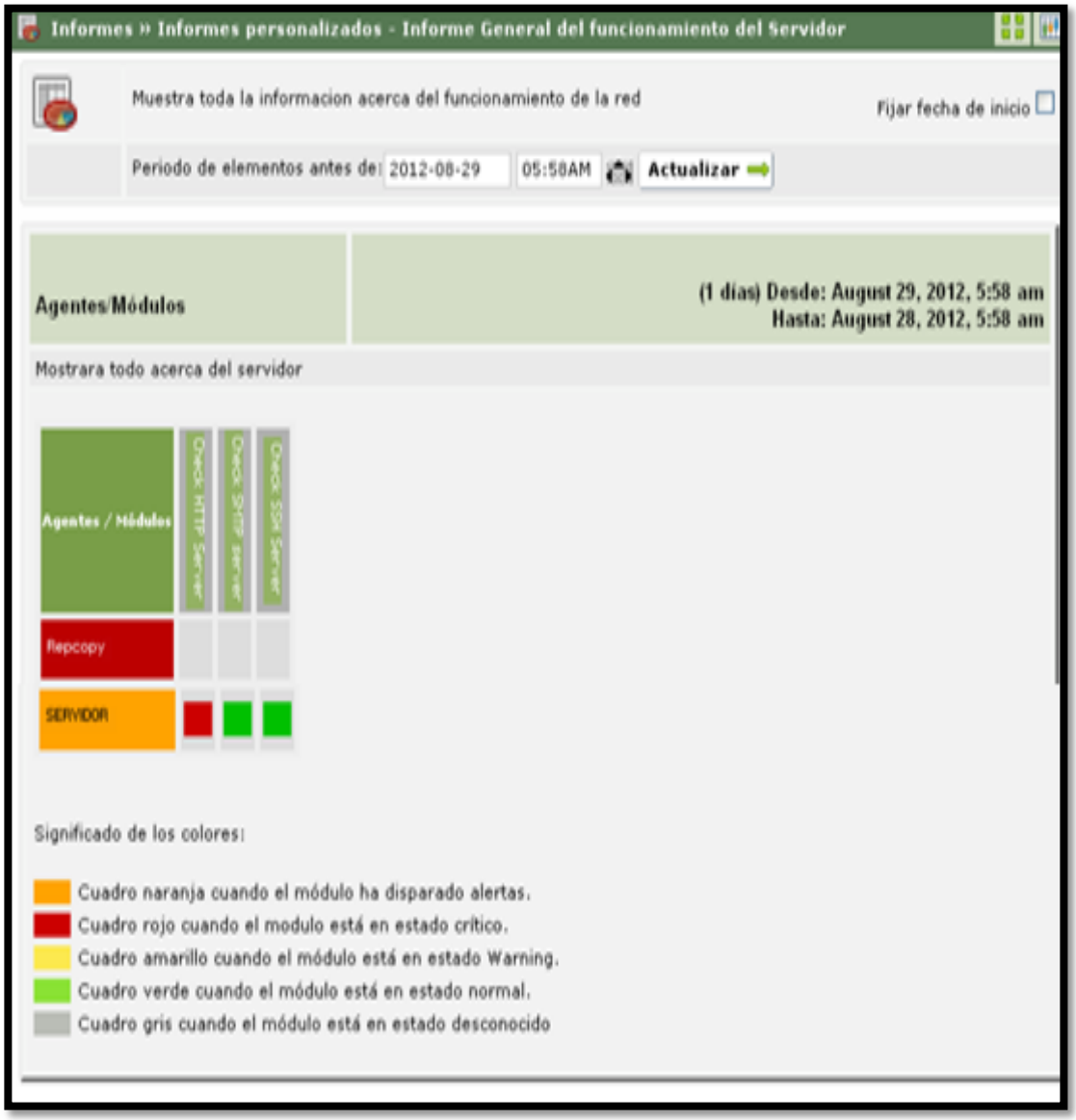


Figura 55: Vista de informes

Autor: William Pullutaxi

6.7. Conclusiones y recomendaciones

6.7.1. Conclusiones

- Al realizar un análisis sobre la vulnerabilidad de la Empresa, es alarmante darse cuenta que hay Empresas como Repcopy que no cuentan con un servicio de alta seguridad en su servidor poniendo en riesgo los datos confidenciales puesto que la Empresa no cuenta con las medidas necesarias de seguridad informática.

- En el Área de Tecnologías Informática existe muchos mecanismos de salvaguardar la información, el principal riesgo es la falta de conocimiento sobre estos, ya que día a día aparecen nuevas herramientas de monitoreo de la red al igual que aparecen las amenazas.

- El Software Pandora FMS, ayuda a enfocar el problema de la seguridad, enfocándose en software y hardware, dando mayor seguridad en la información haciendo de esta confiable y precisa.

- La aplicación de un software con su respectiva tecnología para la detección de intrusiones, para cualquier Institución pública o privada que dependa de una red es importante a la hora de salvaguardar la información, misma que permitirá disminuir la vulnerabilidad de la red.

- La utilización de un software de detección de amenazas disminuye en gran parte la vulnerabilidad de la red, dando confianza y seguridad al momento de hacer uso de cada uno de los elementos de la red al igual que los datos.

6.7.2. Recomendaciones

- Es recomendable la revisión periódica de las amenazas y riesgos ya que la tecnología va cambiando constantemente y deben ser controlados para evitar futuros problemas.

- Realizar la implantación de los Mecanismos de seguridad existentes para tener un control adecuado de la información manejada dentro de la Institución en el Área de Tecnologías de la Información.

- El constante estudio e investigación de las herramientas que ayuden a proteger la red Empresarial será de gran ayuda para en lo futuro no ser víctima de un fraude informático.

- Los riegos y las seguridades de cada Empresa se deben revisar periódicamente como una parte importante de la Empresa tomando en cuenta la tecnología de Seguridad Informática existente.

- La utilización de herramientas de seguridad no son 100% seguras, ya que día a día los delincuentes informáticos estudian la mínima vulnerabilidad de la red y sistemas de detección de amenazas, es por esto que la investigación diaria de nuevas formas de salvaguardar la información será la mejor herramienta para poder protegerse de las amenazas que día a día van apareciendo

Bibliografía

Libros

- GONZALO, Asensio (2006). Seguridad en Internet.Una guía práctica y eficaz para proteger. Primera Edición. Ediciones Nowtilus, S.L. Madrid.

- GONZÁLES, Diego (2003). Sistemas de detección de Intrusiones. Primera Edición, Madrid.

Tesis:

- MIRA Alfaro, Emilio José (2000), Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Universidad de Valencia. España

- NOBLE Benítez Zully Geomara (Marzo, 2008), Desarrollo de u n agente inteligente para pronósticos meteorológicos usando Web services

Leyes

- Constitución de la República del Ecuador. Registro oficial No. 449 del 20 de Octubre 2008.

Internet

- Dra. AMANDI, Analía ("s.f."). Tecnología de Agentes Inteligentes. Disponible en: http://www.exa.unicen.edu.ar/catedras/knowmanage/apuntes/KM-agentes.pdf

- **BORGHELLO, Cristian (2000 – 2009).** Detección de Intrusos en Tiempo Real. Disponible en:

  http://tesis%20parecidas/Seguridad%20Informatica%20-%20IDS%20-%20Detecci%C3%B3n%20de%20Intrusos%20en%20Tiempo%20Real.htm

- Wikipedia®. (2011). Seguridad de la información. 26 de Octubre de 2011. Disponible en:
  http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

- SlideShare Inc. (2011). Que es Seguridad de la Información. 26 de Octubre de 2011. Disponible en:
  http://www.slideshare.net/vaceituno/queesseguridad-fist

- Foundation for Intelligent Physical Agents, "Foundation for Intelligent Physical Agents.Specifications.1997". Disponible en :
  http://www.fipa.org

- GÓMEZ, Juan Camilo (Medellín 2010). Sistema de Monitoreo Pandora. Disponible en: http://www.pandoera/pandora.htm

- ÁRTICA, Soluciones Tecnológicas (Octubre 2010), Manual de Administración de Pandora FMS. Primera Edición. Escrita por:

  - Sancho Larrea Urrea
  - David Villanueva Jiménez
  - Jorge Gonzáles Gonzáles
  - Julia Lerena Urrea (Traducción)
  - Pablo de la Concepción
  - Ramón Novoa
  - Miguel de Dios
  - Sergio Zarzuelo
  - Darío Rodríguez

Otras aportaciones de diferentes autores están disponibles en la página Web http://pandoraFMS.org

ANEXOS

ANEXO 1: CÓDIGO DE PROCEDIMIENTO PENAL DEL ECUADOR ANTE INFRACCIONES INFORMÁTICAS

INFRACCIONES INFORMÁTICAS	REPRESIÓN	MULTAS
Delitos contra la información protegida (CPP Art. 202)		
Violentando claves o sistemas accede u obtiene información	6 meses a 1 años	$500 a $ 1000
Seguridad nacional o secretos comerciales o industriales	1 a 3 años	$1000 a $1500
Divulgación o utilización fraudulenta	3 a 6 años	$2000 a $10000
Divulgación o utilización fraudulenta de custodios	6 a 9 años	$2000 a $ 10000
Obtención y uso no autorizados	2 meses a 2 años	$1000 a $2000
Destrucción de documentos (CPP Art. 262)	3 a 6 años	----------
Falsificación Electrónica (CPP Art. 353)	3 a 6 años	----------
Daños Informáticos (CPP Art. 415)		
Daño dolosamente	6 meses a 3 años	$60 a $150
Servicio público o vinculado con la defensa nacional	3 a 5 años	$200 a $600
No delito mayor	8 meses a 4 años	$200 a $600
Apropiación ilícita (CPP Art. 553)		
Uso Fraudulento	6 meses a 5 años	$500 a $1000
Uso de medios (claves, tarjetas magnéticas, otros instrumentos)	1 a 5 años	$1000 a $2000
Estafa(CPP Art. 563)	5 años	$500 a $1000
Contravenciones de tercera clase(CPP ART. 606)	2 a 4 días	$7 a $14

Fuente: Código de Procedimiento Penal del Ecuador

ANEXO 2. ENCUESTA

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

LUGAR A ENCUESTAR: Empresa Importadora REPCOPY

OBJETIVO DE LA ENCUESTA: Determinar el grado de protección de la información que maneja en la Empresa

Señores, su verdad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo.

Tras dedicar unos minutos a responder este cuestionario, será usted mismo el que descubra el nivel de protección que la Empresa tiene en el sistema de información que maneja así como las ventajas que puede tener la seguridad de información.

1. **¿Ha tenido en cuenta la posibilidad de perder la información, que no se correcta o que se roben?**

   Si ( ) No ( )

2. **¿Cuenta la Empresa con una política de seguridad?**

   Si ( ) No ( )

3. **¿Existen controles que detecten posibles fallos en la seguridad?**

   Si ( ) No ( )

4. **¿Se hace algún tipo de revisión del sistema de información de forma periódica?**

   Si ( ) No ( )

5. **¿Se ha definido niveles de acceso a los usuarios, es decir a que tienen acceso y a que no?**

   Si ( ) No ( )

6. **¿Existen sistemas operativos servidores, que impiden el acceso a los datos a los usuarios no autorizados?**

   Si ( ) No ( )

7. **¿Se realizan copias de seguridad de la información, con qué frecuencia?**

   Si ( ) No ( )

8. **¿Se ha elaborado un plan de seguridad en la Empresa?**

   Si ( ) No ( )

9. **¿Existe un responsable o responsables que coordinen las medidas de seguridad?**

   Si ( ) No ( )

10. **¿Tiene la Empresa elaborado un plan de contingencia?**

    Si ( ) No ( )

11. ¿Existe un presupuesto asignado para la seguridad en la Empresa?

Si ( ) No ( )

12. ¿Existe una política definida para los accesos a Internet?

Si ( ) No ( )

13. ¿Se revisan las páginas accedidas para tomar medidas contra los usuarios que no cumplan sus funciones?

Si ( ) No ( )

14. ¿Dispone la Empresa de herramientas o sistemas que detecten los intentos de acceso a la red de la Empresa?

Si ( ) No ( )

Gracias por su colaboración

Fecha de aplicación

ANEXO 3. GLOSARIO DE TERMINOS

A menudo una de las cosas que más cuesta entender cuando se comienza con Pandora FMS son los términos que se manejan. Si se viene de otro sistema de monitorización o si no se conoce ninguno anterior, resulta bastante confuso. El propósito de este glosario es unificar y definir de forma pormenorizada todas las definiciones de términos comúnmente empleados en Pandora FMS

Agente

Un agente en Pandora FMS es una entidad organizativa, que generalmente suele ser una máquina, sistema o host (un ordenador). El agente contiene información, y pertenece a un grupo (a un único grupo). Un agente también puede ser una unidad organizativa, diferente de un ordenador, puede ser un edificio, un vehículo o cualquier otra cosa que contiene información. El agente contiene información en diferentes módulos. El agente puede estar relacionado con otros agentes, mediante una relación de parentesco (un agente puede ser hijo de otro agente). El agente por tanto es una unidad organizativa dentro de Pandora FMS, un concepto donde se almacena información otras unidades de información llamadas módulos.

Agente software

Aunque se llama igual que el concepto anterior, el agente software hace referencia al programa que se instala en los ordenadores para recoger información de forma automática, ese programa es el llamado "Agente de Pandora FMS" que se instala en todo tipo de sistemas: Windows, UNIX, etc. El agente software es una aplicación que genera un fichero de datos que se envía al servidor de Pandora FMS a través de la red, generalmente usando el protocolo Tentacle.

ACL

ACL es un acrónimo en inglés de Access Control List, o Listas de Control de Accesos (LCA en Español), que en Pandora FMS se definen asignando a un usuario un perfil sobre un grupo.

Acción

La acción es una de las partes de la alerta. Las acciones son instancias (es decir, la particularización) de un comando. Esta particularización hace que las acciones incluyan parámetros específicos. Por ejemplo, sobre el comando **eMail** podríamos definir las acciones **Enviar un correo al administrador** y **Enviar un correo a la lista de distribución del proyecto**, definiendo algunos de los campos que tenía el comando, especificando el email del administrador o el de la lista de correo de distribución, siguiendo el ejemplo anterior.

Alerta

Es una instancia de una plantilla de alerta asociada a un módulo concreto. Puede llevar asociadas distintas acciones y tiene dos estados posibles, disparada o no disparada. La alerta en Pandora FMS, es lo que hace que cuando ocurra algo por ejemplo cuando se cae un servidor, Pandora FMS lo interprete y envíe un email o un SMS a una persona indicándole lo sucedido.

Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.

Análisis de Riesgos: Proceso que permite la identificación de las amenazas que acechan a los distintos activos del sistema de información para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

Ataque: Amenaza de origen intencionado.

Base de datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. Pandora FMS utiliza bases de datos relacionales, en las que el lugar y la forma en que se almacenen los datos no tienen relevancia y se accede a ellos a través de un lenguaje estructurado de consultas estándar (SQL).

Comando: Es otro componente de las alertas de Pandora FMS. Exceptuando los comandos internos de Pandora FMS, que permiten generar eventos, enviar emails etc. un comando representa un programa o utilidad externa que el servidor ejecuta.

Consola o consola WEB: es la aplicación WEB que permite gestionar Pandora FMS mediante WEB.

Confidencialidad: Condición de seguridad que garantiza que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Disponibilidad: Situación que se produce cuando se puede acceder a la información contenida en un Sistema, a sus recursos y servicios, conforme a las especificaciones del mismo. Previene contra la denegación no autorizada de acceso a la información o sistemas.

Esquema de base de datos: Describe la estructura de una base de datos en un lenguaje formal. En una base de datos relacional el esquema define las tablas, los campos de cada tabla y las relaciones entre campos y tablas.

Estado: Normalmente nos referimos al estado de un módulo. Nos da información acerca del módulo en el momento actual. El estado de un agente viene dado por el peor de los estados de sus módulos en conjunto (si tiene 5 modulos y uno está en CRITICAL, dos en WARNING y dos en NORMAL) el estado del módulo sería CRITICAL. Lo mismo se aplica para el estado de un grupo.

Estado CRITICAL, WARNING

NORMAL, WARNING y CRITICAL son los tres estados posibles de un módulo. Los estados WARNING y CRITICAL suelen indicar condiciones de error de distinta gravedad. Pandora FMS permite definir de forma independiente distintos umbrales para los estados WARNING y CRITICAL de cada módulo.

Estado desconocido: Decimos que un módulo está en estado desconocido si no recibe datos desde hace más del doble de su intervalo. Es decir, un módulo que envía datos cada 5 minutos se marca como desconocido después de 10 minutos sin recibir datos. Sin embargo el módulo sigue conservando su estado NORMAL, WARNING o CRITICAL en función del último dato que llegase.

Exploit (del inglés *to exploit*, *explotar* o *aprovechar*) es una pieza de software, o una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado)

Falso positivo/negativo: Cuando un chequeo devuelve un error y éste no se ha producido hablamos de falso positivos. Cuando no devuelve ningún error y éste se ha producido hablamos de falso negativo. Por ejemplo, tenemos un falso positivo si un módulo que devuelve 1 cuando un servidor está disponible y 0 cuando no lo está devuelve 1 sin estar el servidor disponible.

Ficheros de datos / XML de datos: Un XML es un fichero de datos que generan los agentes software de Pandora FMS. Además de la información de los módulos del agente contiene información sobre el propio agente (versión, sistema operativo etc.). El formato XML es un standard en la informática y sirve como contenedor de datos, para más información sobre el formato XML, visitar

http://es.wikipedia.org/wiki/Extensible_Markup_Language.

Fluxbox: es un gestor de ventanas para el Sistema X Window basado en Blackbox 0.61.1. Su objetivo es ser ligero y altamente personalizable, con sólo un soporte mínimo para iconos, gráficos, y sólo capacidades básicas de estilo para la interfaz. Se utilizan atajos de teclado, tabs, y menús simples como interfaces, los cuales pueden ser editados. Algunos usuarios prefieren Fluxbox sobre otros gestores de ventanas debido a su velocidad y simplicidad.

GNOME: es un entorno de escritorio e infraestructura de desarrollo para sistemas operativos Unix y derivados Unix como GNU/Linux, BSD o Solaris; compuesto enteramente de software libre.

Grupo: es un elemento organizativo. Los grupos contienen agentes, y los grupos se usan como referencia para establecer que cosas puede ver y que no puede ver un usuario. Por ejemplo, cuando se define un informe y este está relacionado con un grupo, solo los usuarios con acceso a ese grupo pueden ver ese informe.

Los grupos pueden contener otros grupos, pero esa jerarquía no se ve (al menos en la versión 3.1 y anteriores) de ninguna otra manera ni se tiene en cuenta en el sistema de permisos.

Impacto: Consecuencia sobre un activo de la materialización de una amenaza.

Incidente: Cualquier evento no esperado o no deseado que pueda comprometer la seguridad del sistema.

Integridad: Condición de seguridad que garantiza que la información/sistema no ha sido modificada o alterada por personas, entidades o procesos no autorizados.

KDE: es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

Módulo: Un módulo es una entidad atómica de información que almacena valores (numéricos, o de tipo alfanumérico/texto). Cada módulo sólo almacena un tipo de dato, del mismo tipo. Es decir, un módulo que almacena el caudal de tráfico en un

router, solo almacena ese valor (números que se van incrementando en el tiempo). Los agentes están contenidos dentro de los agentes, y siempre asociados a un único agente. Un agente puede contener N módulos. Los módulos no están relacionados entre sí.

Monitor

Es un módulo con un estado asociado. En versiones anteriores de Pandora FMS únicamente los módulos booleanos tenían estado (normal cuando estaban a 1 y crítico cuando estaban a 0). Actualmente todos los módulos permiten definir umbrales para tres estados diferentes. Cuando un módulo no tiene información de estado asociado, no sabe cuándo ponerse crítico o en warning, de forma que es simplemente un módulo.

Monitorización síncrona

Decimos que un módulo es síncrono cuando devuelve datos a intervalos regulares. Por ejemplo, una medición de temperatura cada 5 minutos.

Monitorización asíncrona

Decimos que un módulo es asíncrono cuando devuelve datos en función de su disponibilidad. Por ejemplo, buscar una cadena en un fichero de log. Si no se encuentra la cadena, el módulo no devuelve datos. Otro ejemplo -muy frecuente- es el de los traps SNMP, que sólo se generan cuando ocurre un error (por ejemplo, fallo en una fuente de alimentación).

Paquete

Un paquete contiene un programa o conjunto de programas empaquetados en un determinado formato listo para ser instalado en un sistema operativo y versión determinados. Por ejemplo, un paquete RPM para OpenSUSE Linux.

Plantilla de alerta

Es uno de los tres componentes de las alertas. Define la configuración de una alerta de forma general (llamaremos alerta propiamente dicha a la instancia de una plantilla). Permite especificar la condición de disparo, que puede depender del valor o del estado de un módulo, y otros detalles como el número máximo de veces que se disparará en un intervalo dado o las opciones de recuperación.

Perfil

Es un grupo de "permisos" sobre diferentes operaciones posibles en Pandora FMS: ver un agente, modificar un agente, asignar alertas, definir informes, gestionar la BBDD, etc.

Política de seguridad: Conjunto de reglas, directivas y prácticas que gobiernan cómo se gestionan, protegen los activos y recursos de información.

Protección Flip/Flop

La protección flip flop de un módulo indica el número de veces que se debe dar la condición de cambio de estado para que se produzca el cambio de estado. Esto permite proteger a un módulo de falsos positivos/negativos. Por ejemplo, si sabemos que un módulo devuelve falsos positivos, pero nunca más de dos seguidos, podemos configurar la protección de flip flop a tres para evitar que los falsos positivos produzcan cambios de estado.

Riesgo: Posibilidad de que se produzca un impacto determinado en un activo, en un conjunto de activos o en toda la organización causando un daño en alguna de sus dimensiones.

Seguridad: Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar daño a un sistema o a la organización.

Seguridad informática: Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los recursos de información tecnológicos de una organización.
Sniffer: En informática, un **analizador de paquetes** es un programa de captura de las tramas de una red de computadoras.
Servidor remoto: Servidor que está en red y no es el servidor local.

Servidor: El servidor de Pandora FMS es quien procesa la información recolectada de diferentes maneras, también son los que ejecutan alertas y envían los datos a la base de datos. Hay muchos subtipos de servidores de Pandora, y cada uno realiza una operación. Los servidores de tipo red, por ejemplo, realizan pruebas de monitorización remotas (a distancia, mientras que los servidores de datos, procesan XML recogidos).

A veces se habla genéricamente "Servidor" cuando nos referimos a un sistema, a un ordenador.

Shell o línea de comando: Interfaz que permite la introducción de comandos por medio del teclado.

SVN / Subversion / Repositorio de código: Es un sistema de control de versiones que guarda un repositorio con las distintas versiones de los archivos que integran un proyecto a lo largo de su vida. Al conjunto de archivos en un instante del tiempo dado se le denomina revisión, de modo que dos personas que tengan la misma revisión del proyecto tendrán dos copias idénticas de los mismos archivos.

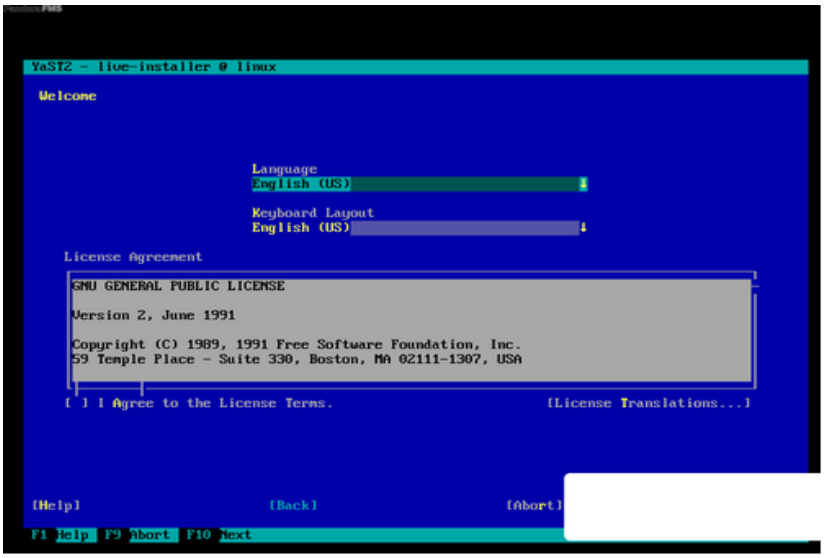
Umbral de alerta (Alert threshold): Es el intervalo de tiempo en el que aplican las restricciones definidas al configurar la plantilla de la alerta. Por ejemplo, una plantilla de alertas que defina un umbral de 10 minutos y un número máximo de alertas de 5, garantiza que en un intervalo de 10 minutos la alerta no se disparará más de 5 veces.

ANEXO 4: INSTALACION DE PANDORA FMS

A continuación se detallara los pasos de instalación:

Lo primero que tendrá que hacer es verificar que la configuración del BIOS de su servidor arranque desde CD. Debería ver una pantalla similar a la siguiente, y pulsar la primera opción:

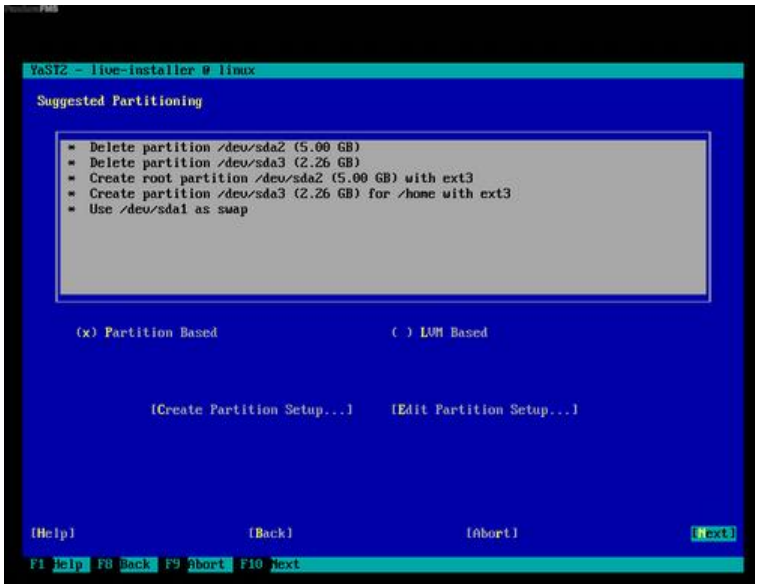
Después de unos segundos, o un par de minutos a lo máximo, nos mostrará la pantalla de bienvenida similar a la siguiente imagen y de aceptación de la licencia GPL. En todas las pantallas, pulsando F10 avanzaremos hacia delante. En esta pantalla de bienvenida hay que marcar la casilla "Aceptar", por lo cual nos desplazaremos por los menús con la tecla TAB y marcaremos las casillas de "marcar / desmarcar" con el espacio:



La siguiente pantalla nos permite elegir la zona horaria. No tiene especial interés ni dificultad. Elija su zona horaria y pulse aceptar o F10.

- **Particionamiento de disco**

La siguiente pantalla, de especial importancia, nos permite particionar el disco. Por defecto el sistema opta por un sistema mixto de Particionamiento físico, que deja la mayor parte de espacio para la partición raíz. En la mayoría de los sistemas esto es más que aceptable, por lo que pulsaremos F10.

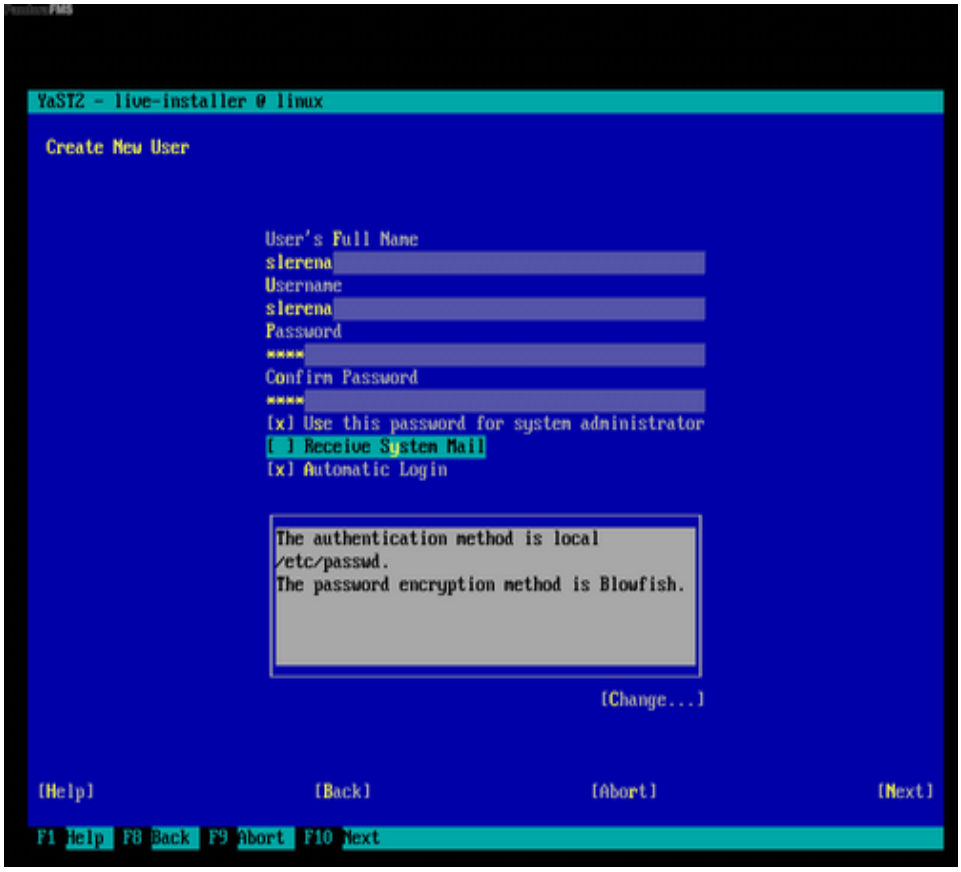


- **Creación de usuario**

Debe crear un usuario. Con el podrá acceder al sistema remotamente por SSH, y hacerse root mediante el uso del comando:

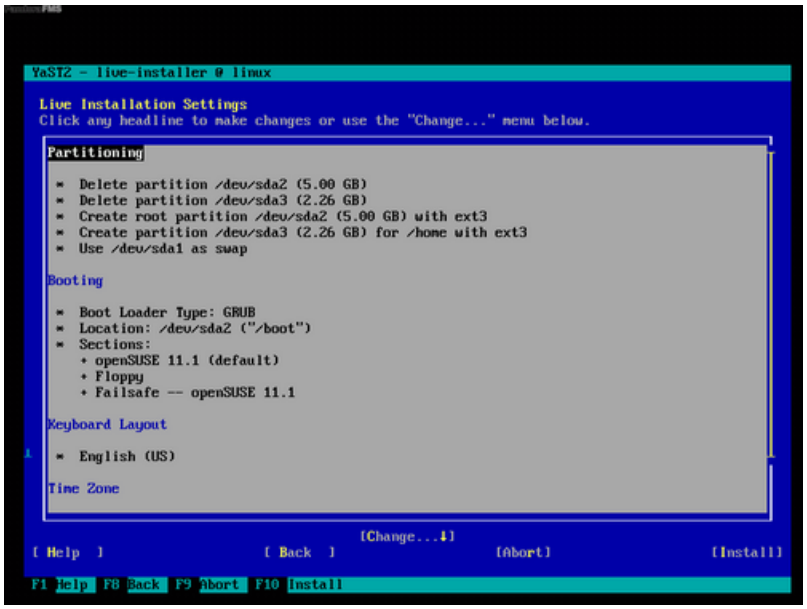
sudo -s

Es importante destacar que el sistema viene securizado de forma que el usuario Root no puede acceder remotamente, por lo que crear una cuenta y recordar la password es esencial.

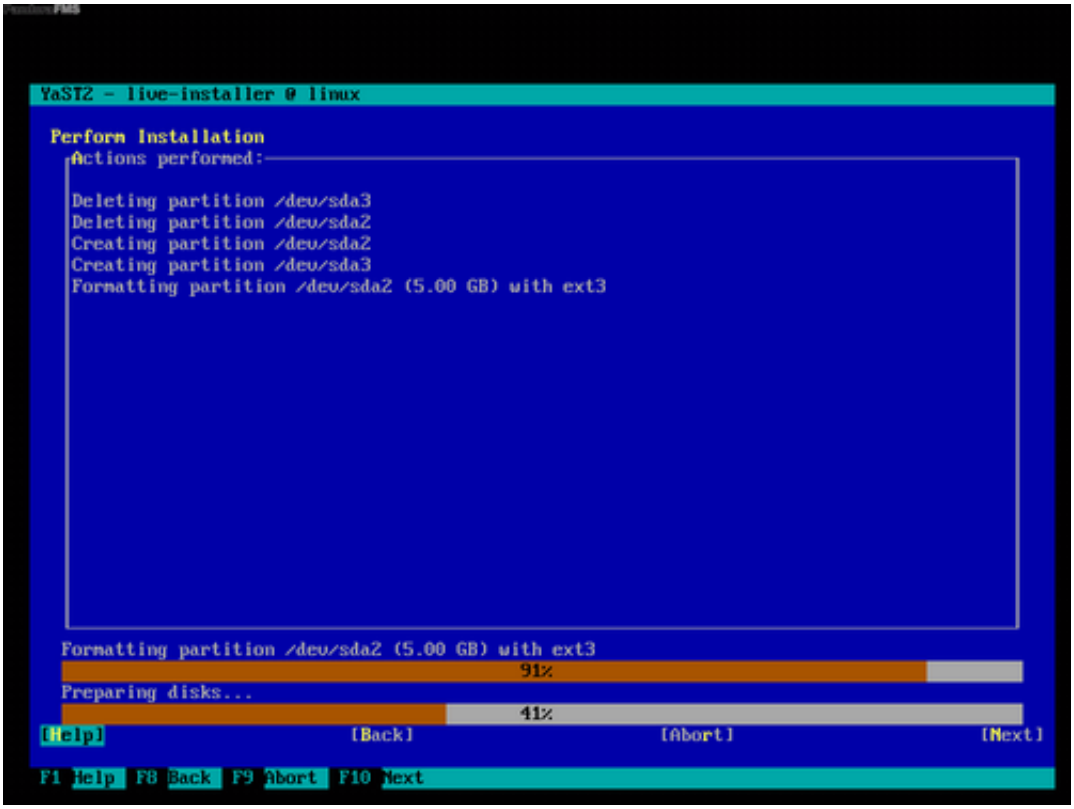


- **Preparación de la instalación (sólo usando imagen ISO)**

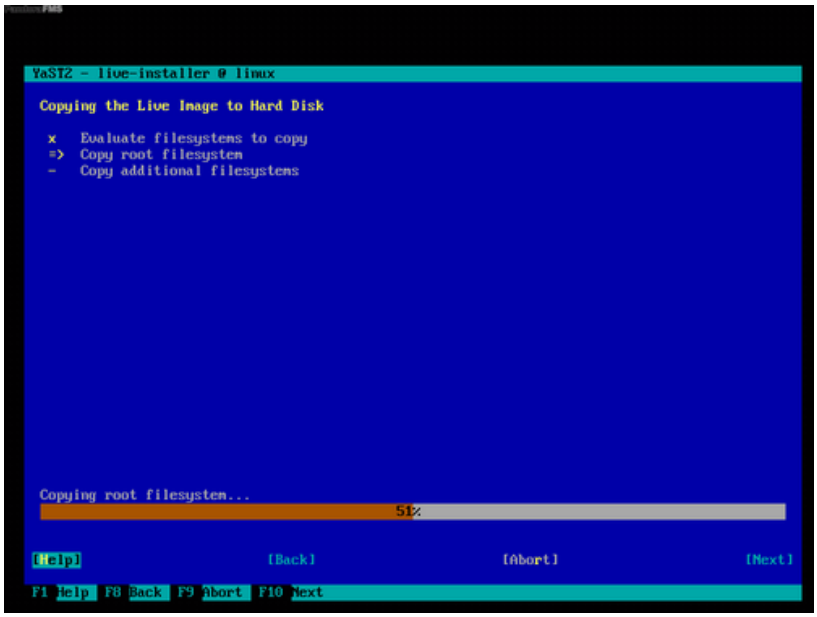
El sistema le mostrará por pantalla un "resumen" de toda la instalación, debe revisarla y aceptarla, pulsando F10 para comenzar la instalación:



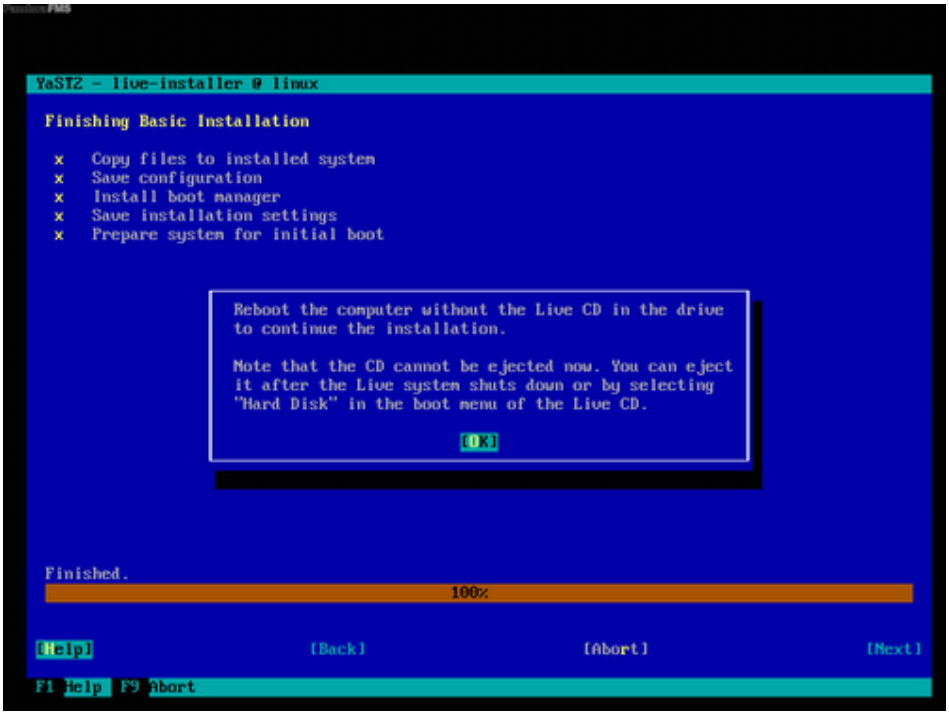
La instalación comenzará, primero creando la estructura del disco del sistema.



Y posteriormente instalando el sistema completo.



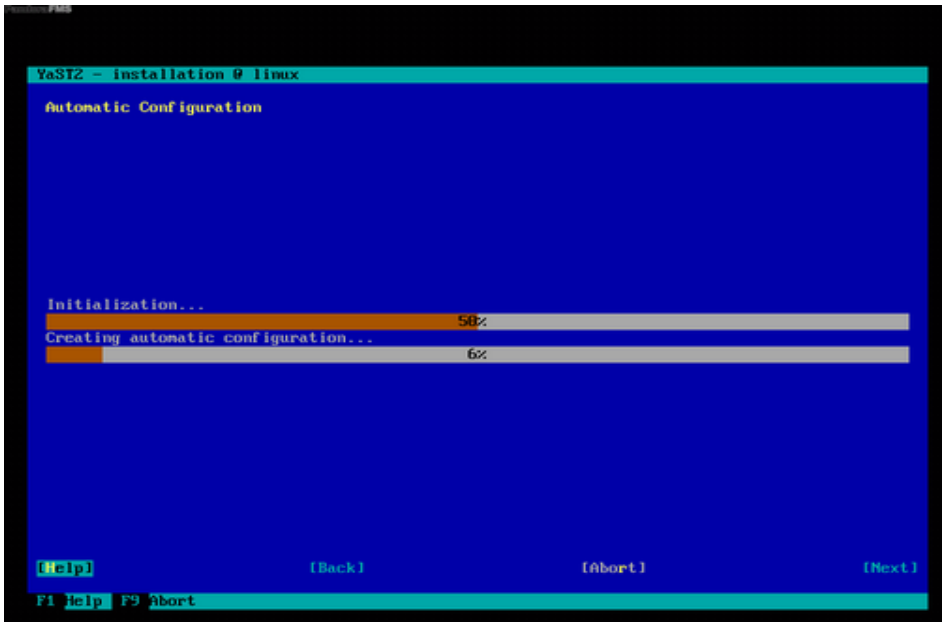
Y finalmente, cerrando la instalación. Al final de este proceso, le pedirá que reinicie el sistema **y que retire el CD** de la unidad, para que el sistema pueda arrancar el sistema recién instalado desde el Disco Duro.



- **Primer inicio**

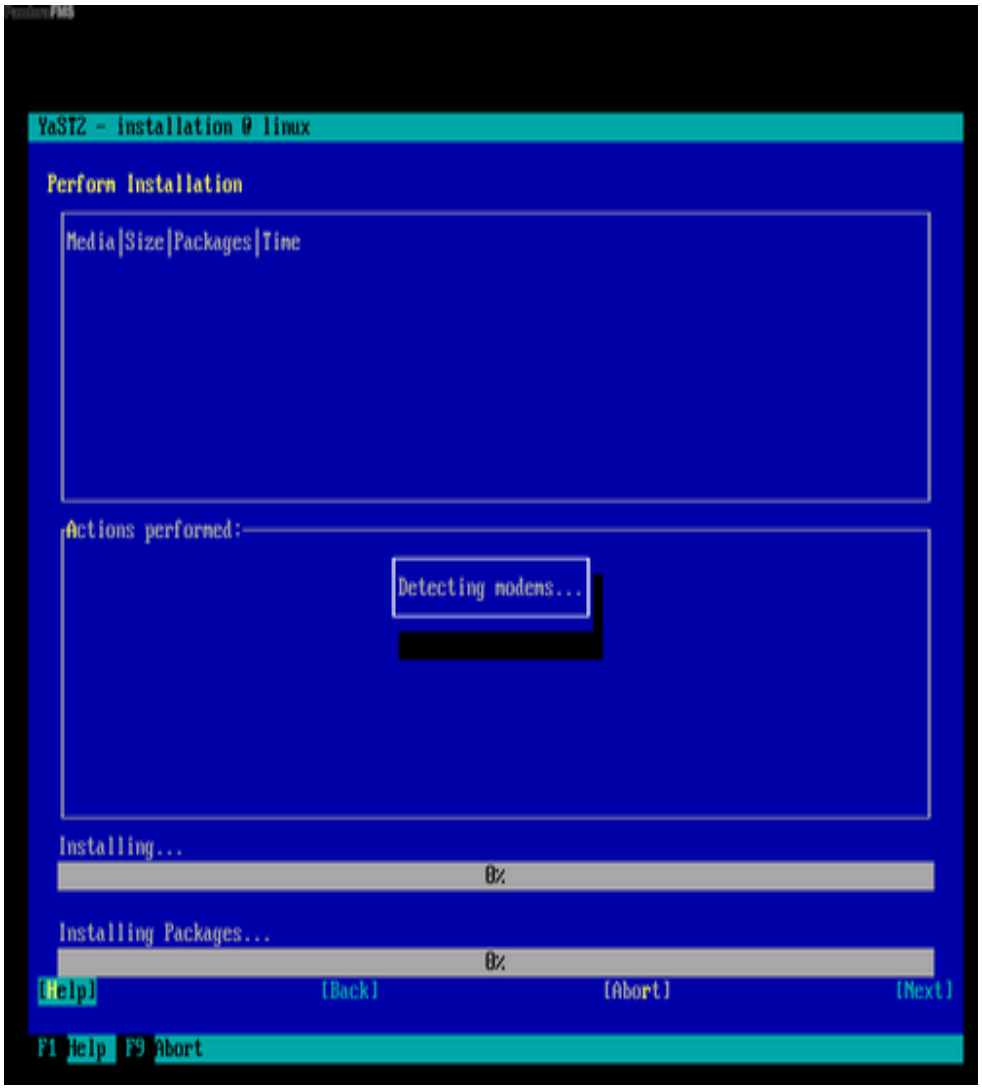
El sistema arrancará por primera vez y nos permitirá configurar algunos parámetros, tales como el idioma, el teclado, y la configuración básica de red (nombre del host, dirección IP, ruta por defecto). Después de eso, arrancará los servicios básicos de Pandora y del sistema (Servidor WEB, base de datos, demonios de Pandora FMS) y el sistema estará listo para su uso.

En el primer inicio, se puede ver una pantalla como la siguiente:



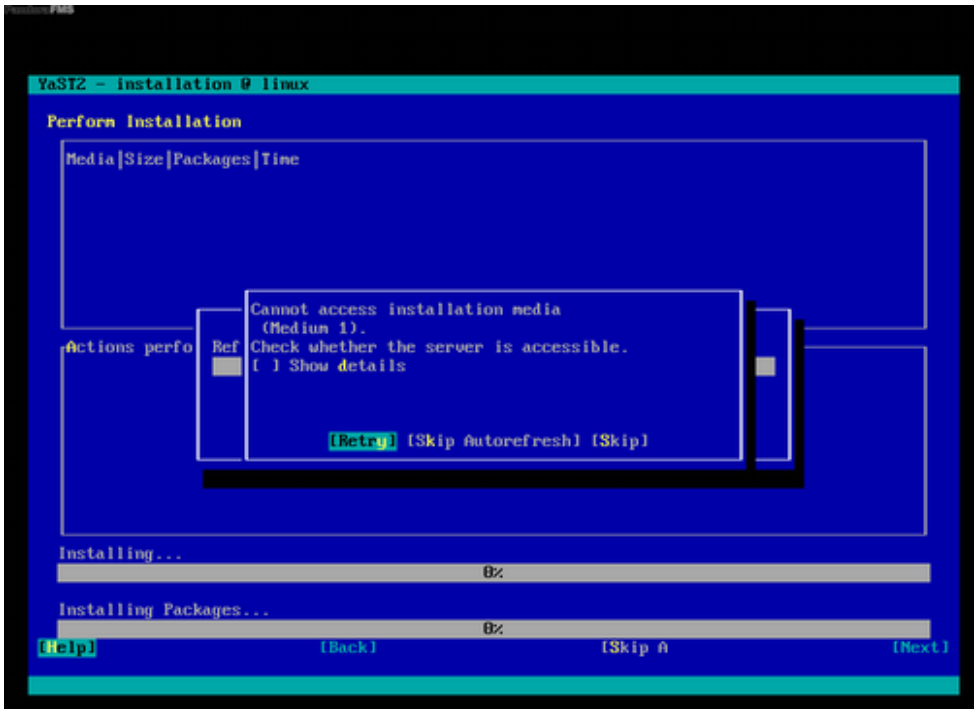
El sistema está detectando conectividad para intentar actualizar los paquetes. Si no la encuentra, no se preocupe, puede dar algún error que deberá ignorar, pero podrá instalar el sistema normalmente utilizando los paquetes ya incluidos en el propio CD. Si tiene conexión directa a Internet el instalador podrá instalar los componentes más actualizados en lugar de los que trae.

Una vez que ha detectado los dispositivos, instalará algunos paquetes adicionales, como se ve en esta pantalla:



En este punto, y dependiendo de la conectividad de que disponga en el servidor donde ha instalado el CD, intentará conectarse a Internet y actualizar los repositorios de software con los que el sistema viene "preconfigurado". En este caso, intentará conectarse, validar las claves de los repositorios y en algunos casos puede que falle al descargar algunos índices.

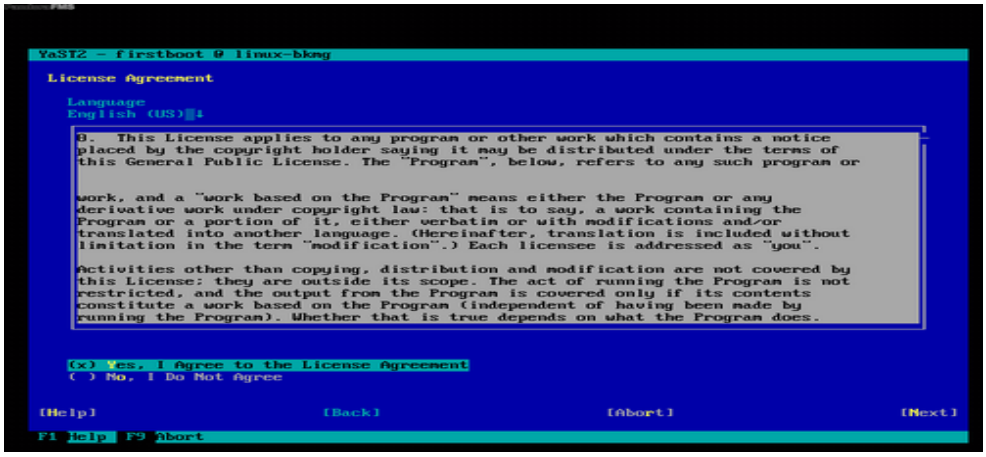
Esta es una pantalla de error al intentar conectar para actualizar los paquetes si no tiene conexión:



Pulse en "Skip Autorefresh" hasta que aborte el proceso de actualización de los repositorios. Siempre podrá actualizar los repositorios más tarde, desde línea de comandos o desde Yast.

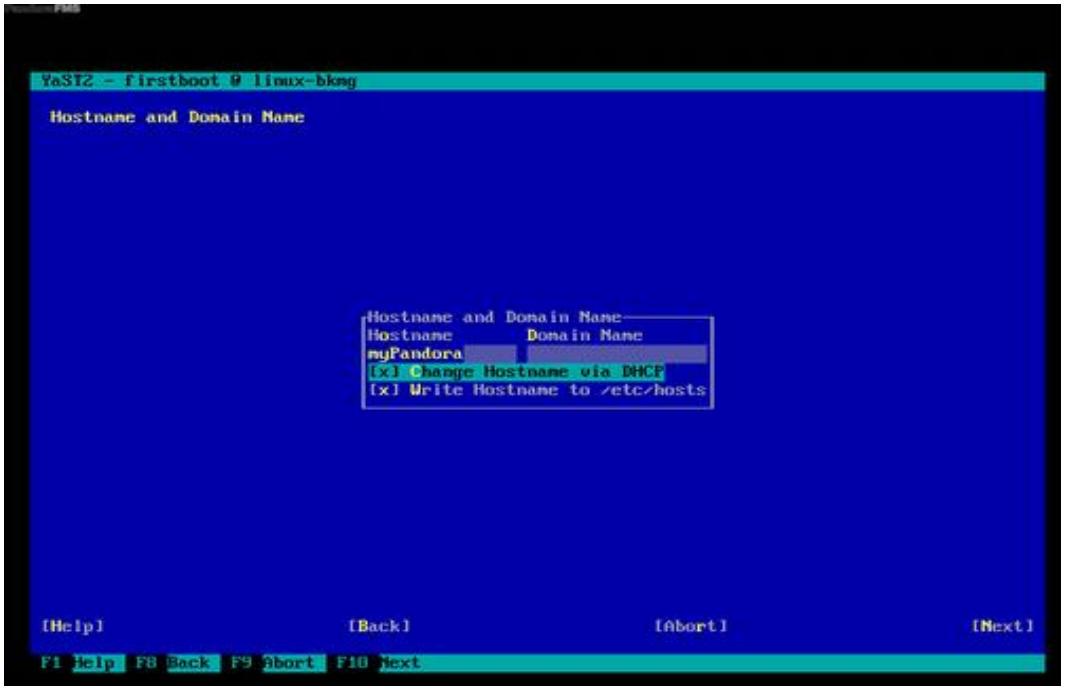
- **Configuración base del sistema**

Empezaremos con la aceptación de la licencia, nuevamente si vienes usando la imagen ISO:

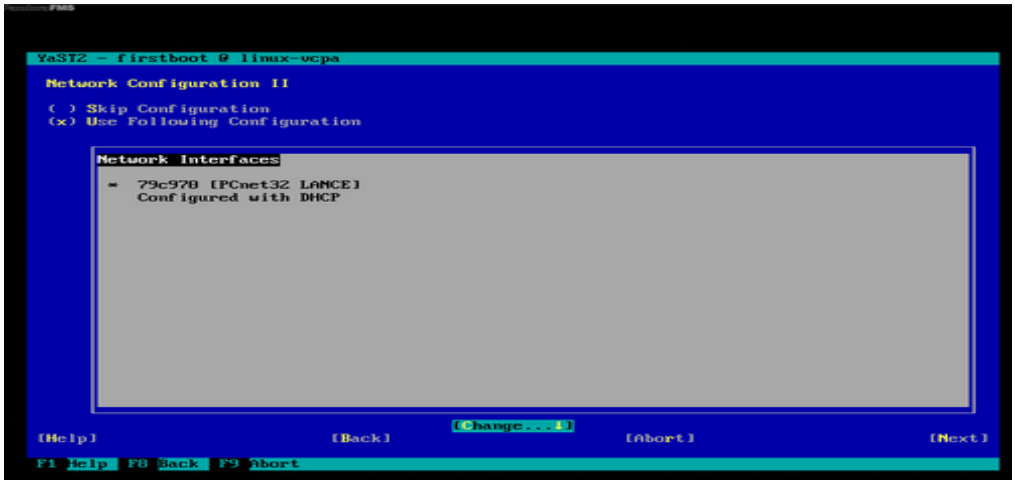


- **Configuración de red**

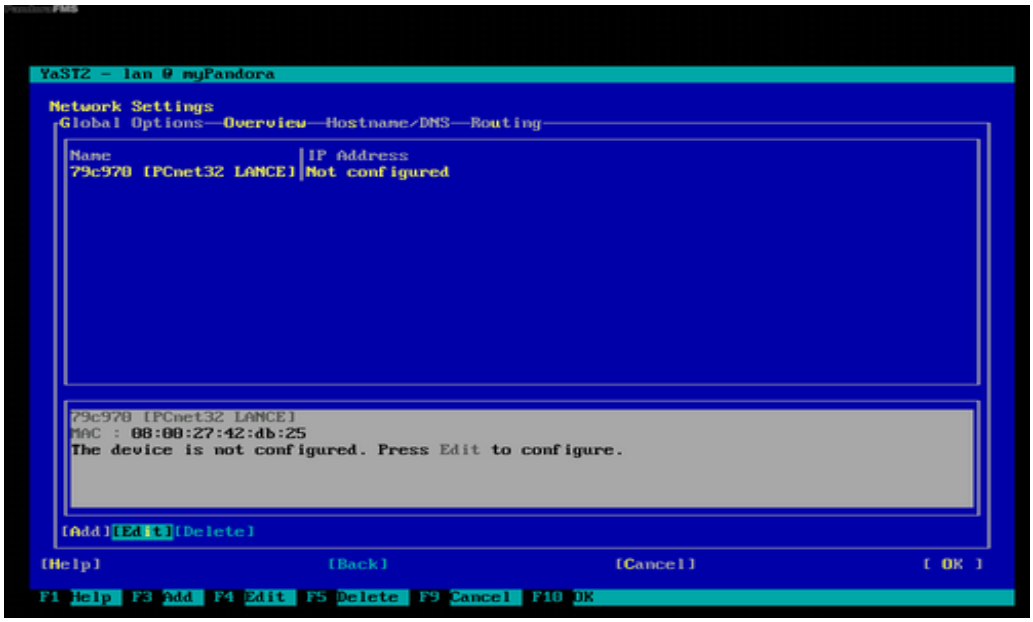
La configuración del hostname del sistema



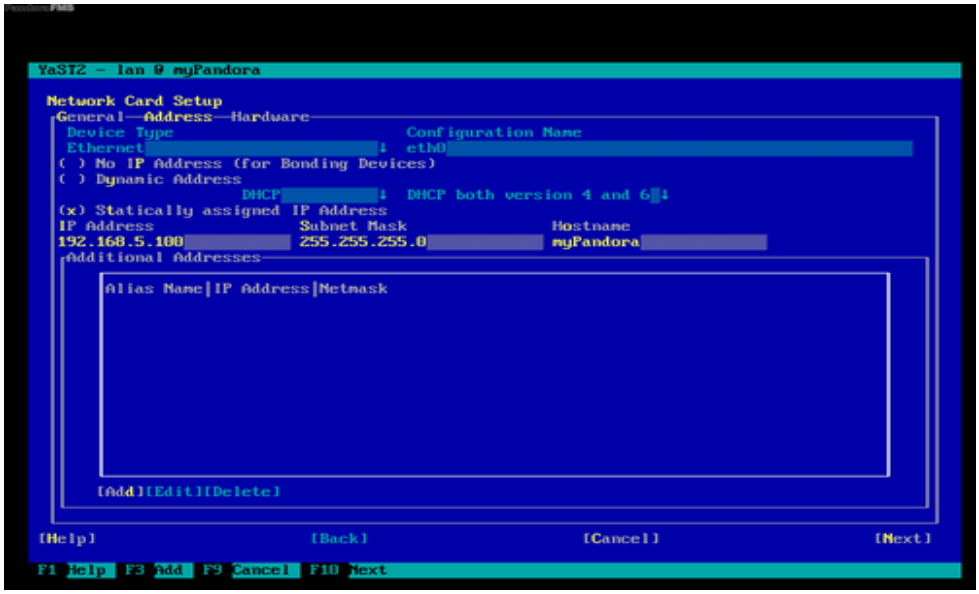
Posteriormente nos mostrará una pantalla con las interfaces de red del sistema. Debemos elegir una para configurarla manualmente, ya que si pulsamos OK o F10, configurará esta con DHCP. Recuerde que se desplaza con TAB entre los campos y escoge el valor pulsando ENTER.



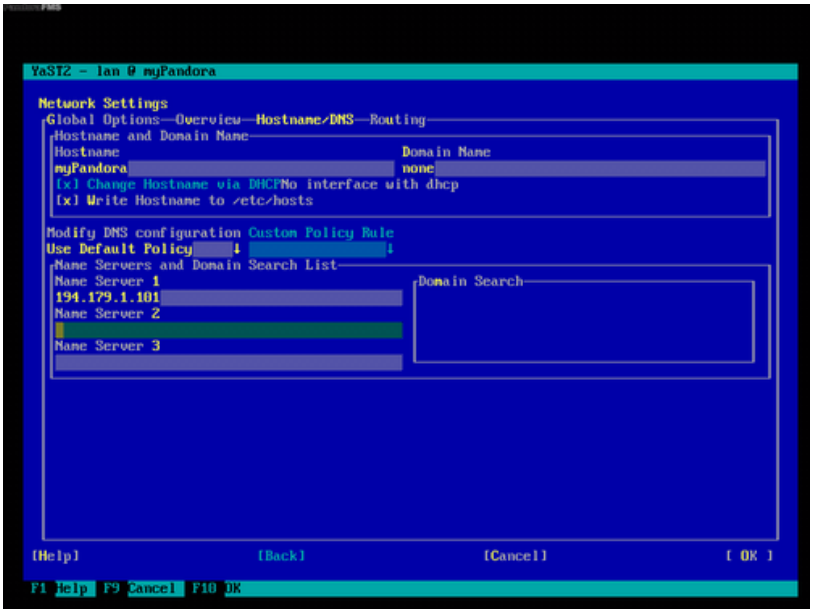
Al elegir configurar la tarjeta de red, nos mostrará una pantalla como la siguiente. Aquí debemos elegir la tarjeta de red, y seleccionar "EDIT" en la caja de abajo. Esto nos llevará a la configuración de red de esa tarjeta de red.



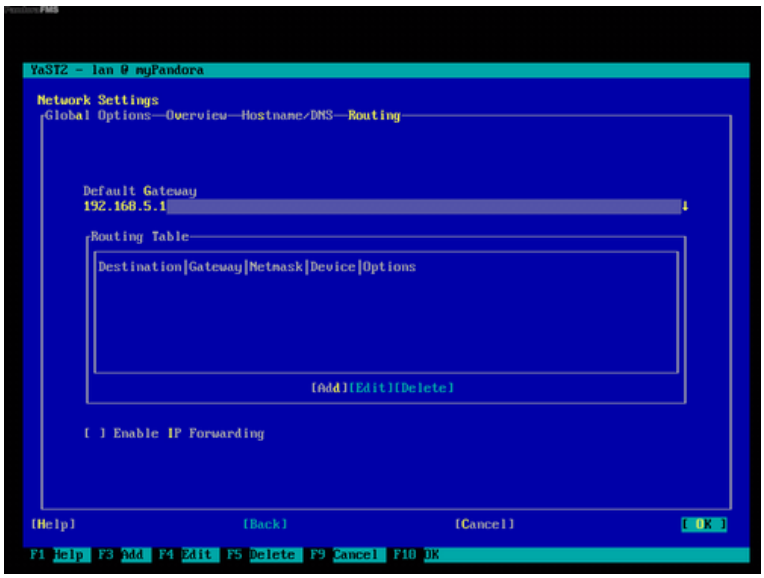
Aquí debemos elegir si queremos IP automática por DHCP o una IP asignada por nosotros. En este ejemplo se ha elegido 192.168.5.111 como IP con mascara de clase C.



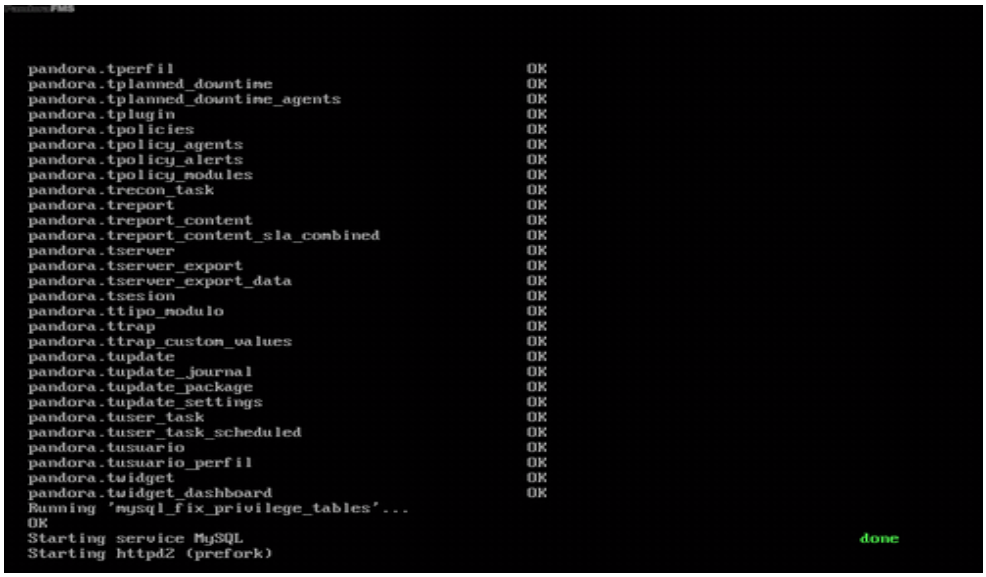
Al pulsar OK, volvemos a la pantalla anterior y podemos movernos a la opción de la derecha con el tabulador, que nos permite configurar los DNS. En esta pantalla hemos utilizado un DNS público, y definido el hostname y el nombre de dominio de la máquina.



Finalmente, en la última opción de la derecha, podemos elegir la ruta por defecto, que en este caso es 192.168.0.1



Finalizada la configuración de red, el sistema salva toda la configuración e inicializa las tablas de Pandora FMS, y arranca los servicios:



El sistema ya está listo. Podemos entrar en el sistema Linux con nuestro usuario o con el usuario root y la password que le hemos definido al usuario que hemos creado antes.

- **Uso de Pandora FMS**

Recuerde que la cuenta "pandora" de MySQL ha sido creada con una contraseña fija. Compruebe su /etc/pandora/pandora_server.conf para ver la contraseña por defecto. También han sido creados otros usuarios fijos: artica y root, y ambos usuarios tienen la misma contraseña fija que tiene el usuario del MySQL de "pandora". Es necesario cambiar tan pronto como le sea posible con los siguientes comandos:

```
passwd root
passwd artica
```

Para cambiar la contraseña de usuario MySQL, hay que ejecutar el comando

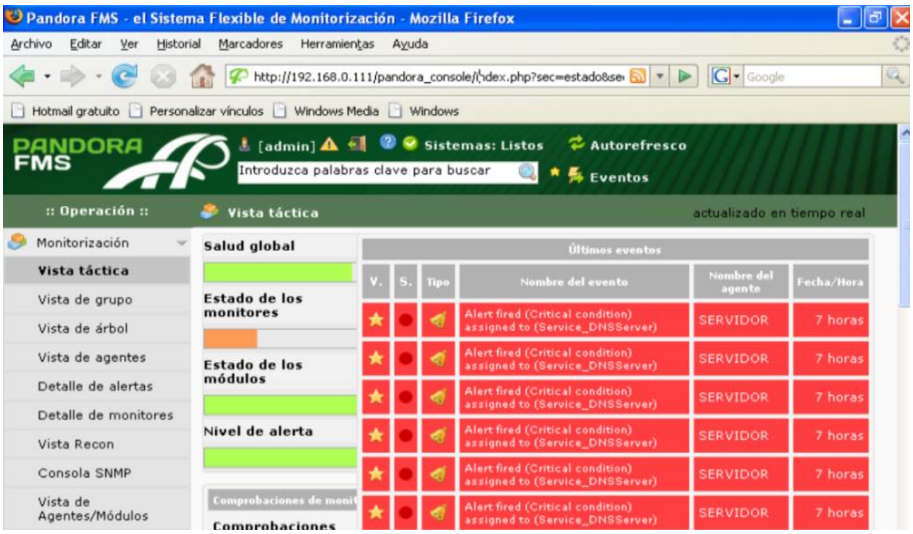
```
mysqladmin -p password pandora
```

El sistema preguntará por el password actual de la cuenta "pandora" antes de cambiarlo. No olvide actualizar /etc/pandora/pandora_server.conf ni tampoco /srv/www/htdocs/pandora_console/include/config.php con la nueva password que haya establecido para la cuenta "pandora" de MySQL.

- **Primera conexión con Pandora FMS**

Simplemente abra un navegador desde otra máquina conectada en red a su servidor recién instalado, y escriba en el la siguiente URL:

http://192.168.0.111/pandora_console



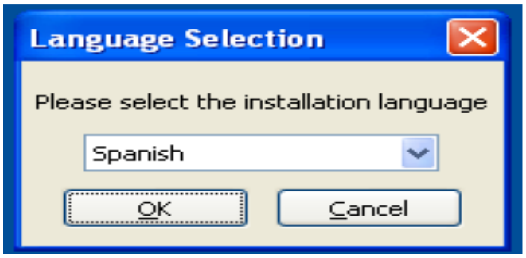
En nuestro caso la dirección ip del servidor de Pandora FMS será 192.168.5.100. A partir de aquí, utilice las credenciales por defecto de Pandora FMS: admin / pandora y puede empezar a trabajar de inmediato con su Servidor de Pandora FMS OpenSuSE.

ANEXO 5: INSTALACIÓN DEL AGENTE WINDOWS

El agente se entrega como un auto instalador en formato ejecutable (.exe). La instalación básica realiza todos los pasos necesarios y tan sólo es necesario aceptar todas las opciones.

Para instalar el agente de Pandora FMS en Windows sólo hace falta descargarlo y ejecutarlo. El instalador le guiará a través de los pasos necesarios en el idioma que seleccione. En el siguiente ejemplo se muestra la instalación para Windows server 2003, recuerde que Pandora FMS funciona en cualquier plataforma moderna de Microsoft (2000 o superior).

- Seleccione el idioma:



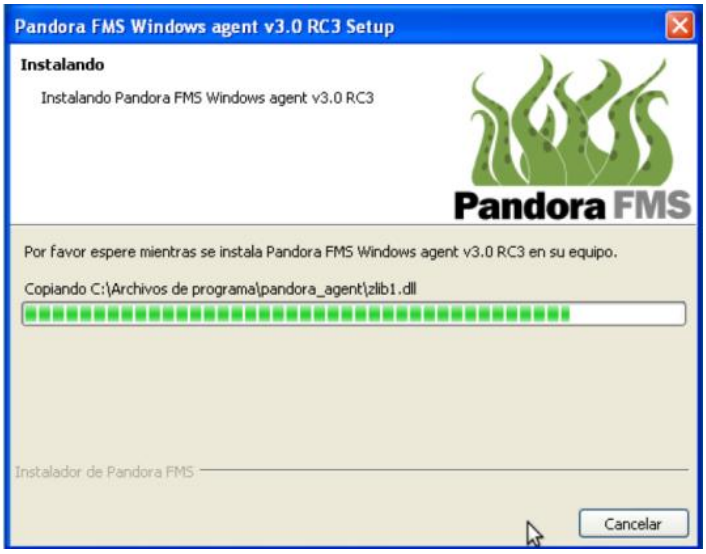
- Siga los pasos del instalador:

- Acepte los términos de la licencia y pulse Next:

- Seleccione la ruta donde se instalará el agente de Pandora FMS (por defecto se instala en c:/archivos de programa/pandora_agent), puede cambiarla pulsando Browse..., después pulse Next:

- Compruebe los datos de instalación y pulse el botón Next:

- Espere a que se copien los ficheros.

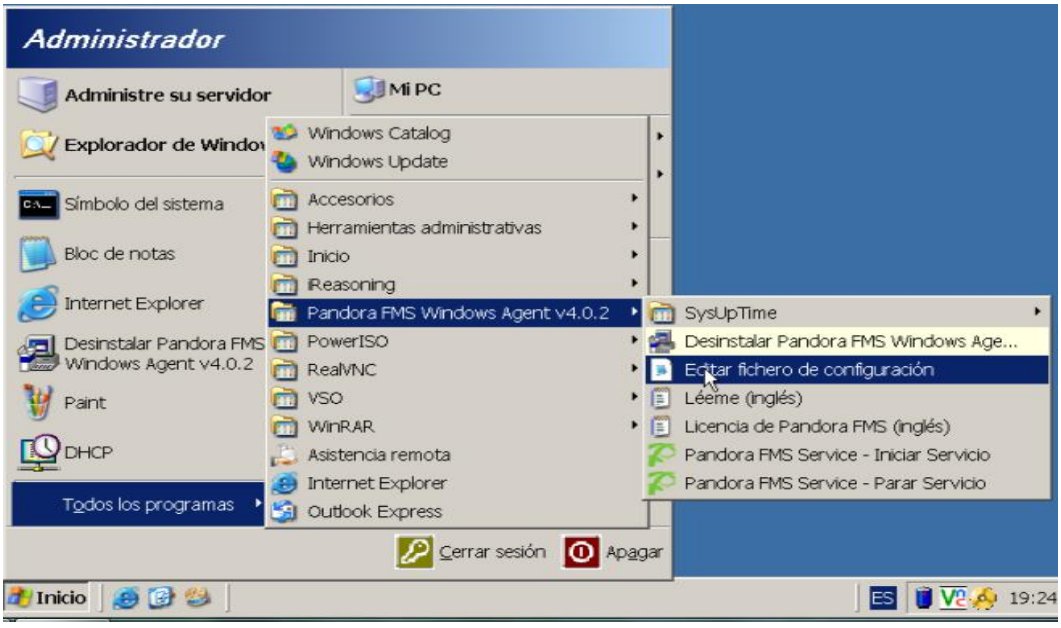


- Configure los datos para el agente como la dirección IP (o nombre) del servidor de Pandora FMS que recibirá los datos del agente. Para poder cambiar otros parámetros, tales como cambiar el nombre del agente (por defecto toma el valor del hostname de la máquina) o la ruta de los ficheros temporales tendrá que editar a mano la configuración del agente.

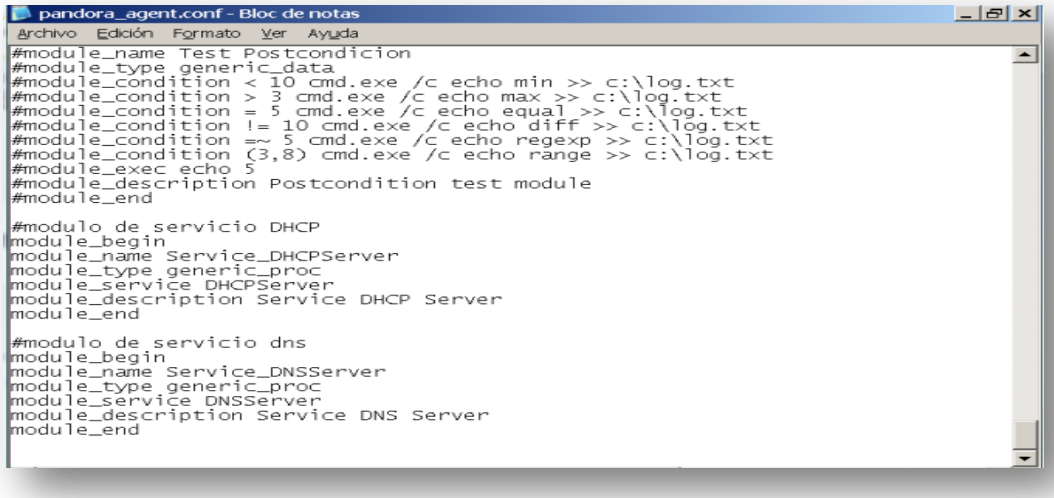
- Decida si quiere iniciar en el momento el servicio del agente de Pandora FMS, de lo contrario tendrá que hacerlo de forma manual, o bien se iniciará cuando Windows se reinicie de nuevo.

- La instalación ha finalizado, puede cambiar los parámetros del agente en el fichero pandora_agent.conf o bien a través del enlace directo en el menú PandoraFMS:

Como hemos mencionado anteriormente el archivo de configuración se almacena en la ruta: c:/archivos de programa/pandora_agent.



Es en este archivo donde se crea los módulos iniciales del agente (maquina) que se iniciara explorando cada máquina en donde se puede agregar más módulos de monitoreo de los servicios.



Como podemos observar en la imagen anterior vemos los módulos creados al momento de la instalación, como ejemplo tenemos la monitorización del módulo para ver si el servicio DHCP está funcionando o no, al igual que un módulo para el servicio DNS mismos que aparecerán en la consola Web de pandora tal como se muestra en la imagen siguiente.

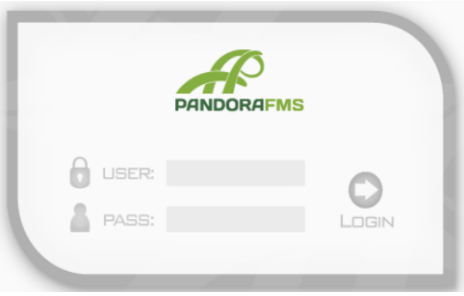
Como podemos observar en los dos gráficos anteriores el nombre de los módulos coinciden en las dos imágenes, por lo tanto son los módulos establecidos en el archivo de configuración del agente pandora pasan a visualizarse en la consola Web de pandora.

ANEXO 6: INTERFAZ DE PANDORA FMS

En este capítulo se proporcionarán las bases de los menús de la interfaz de Pandora FMS, así como de todos los iconos y características necesarias para comenzar a aprender cómo usar Pandora FMS.

- **Pantalla de inicio de sesión de Pandora FMS**

En la siguiente imagen se muestra la pantalla de inicio de sesión de Pandora FMS:



En ella aparece el logotipo de la aplicación. Bajo el logo están las entradas de texto para el usuario y su contraseña, así como el botón de inicio de sesión (Login).
Una vez que se introduzcan las credenciales de inicio de sesión válidas, que por defecto, serían:

- **Usuario**: admin.
- **Contraseña**: pandora

De forma predeterminada, la consola mostrará la página principal de bienvenida de Pandora FMS.

- **Página principal de Pandora FMS**

La página principal de Pandora FMS muestra información básica y general acerca del estado de los sistemas y del número y tipo de comprobaciones que realiza Pandora FMS.
A continuación, se muestra la pantalla principal de Pandora FMS y sus elementos.

Los elementos estáticos que no cambian entre las diferentes pantallas en la interfaz son:

- Menú de Operación
- Menú de Administración
- Enlaces definidos
- Cabecera

Los elementos dinámicos que cambian entre las diferentes pantallas son:

- Noticias del sitio
- Última actividad en la consola Web
- Información del Update Manager
- Información general básica
- Vista general de las comprobaciones en Pandora FMS

- **El menú Operación**

El menú Operación permite visualizar todas las comprobaciones que llevan a cabo los agentes de Pandora FMS, los mapas visuales, los mapas de red, el estado de los

servidores, el inventario, ver y gestionar los incidentes (si se dispone de permisos suficientes), ver los usuarios, ver la consola SNMP, ver los mensajes, y usar las extensiones.

Dentro de cada submenú del menú de Operación, pueden existir otros elementos que se despliegan al seleccionar el menú:

Cada uno de estos elementos proporciona otra página con información. Todas ellas se explicarán en detalle en el anexo de operación con Pandora FMS.

- **El menú Administración**

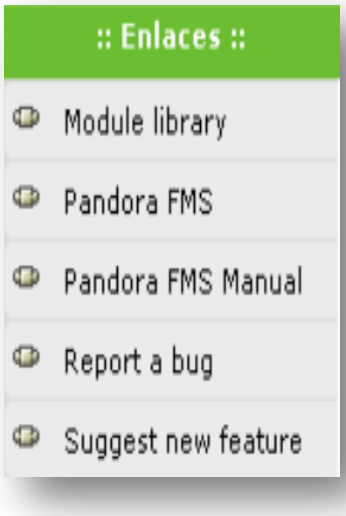
El menú Administración permite visualizar y gestionar las comprobaciones que llevan a cabo los agentes de Pandora FMS, los módulos y componentes de dichas comprobaciones, las alertas que pueden lanzar dichos módulos y agentes y cómo funcionan dichas alertas, las políticas existentes, los usuarios, la consola SNMP, los informes, los perfiles de los usuarios, los servidores de Pandora FMS y sus tareas asignadas, el registro de auditoría del sistema, el comportamiento general de la consola Web de Pandora FMS, el mantenimiento de la base de datos y las extensiones de la consola.

Dentro de cada submenú del menú de Administración pueden existir otros elementos que se despliegan al seleccionar el menú:

Cada uno de estos elementos proporciona otra página con información. Todas ellas se explicarán en detalle en el anexo de operación y gestión con Pandora FMS.

- **El menú Enlaces**

El menú de enlaces simplemente muestra un enlace a sitios pre configurados. Éstos se pueden añadir, modificar y borrar desde el menú de Administración de Pandora FMS. Estos enlaces permiten enlazar Pandora FMS con otras aplicaciones WEB de su organización y hacer que Pandora FMS sea un punto de gestión central.



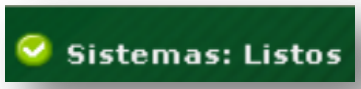
- **La Cabecera**

La cabecera de Pandora FMS ofrece varios enlaces rápidos, o accesos directos, a características importantes del sistema, así como una barra de búsqueda:

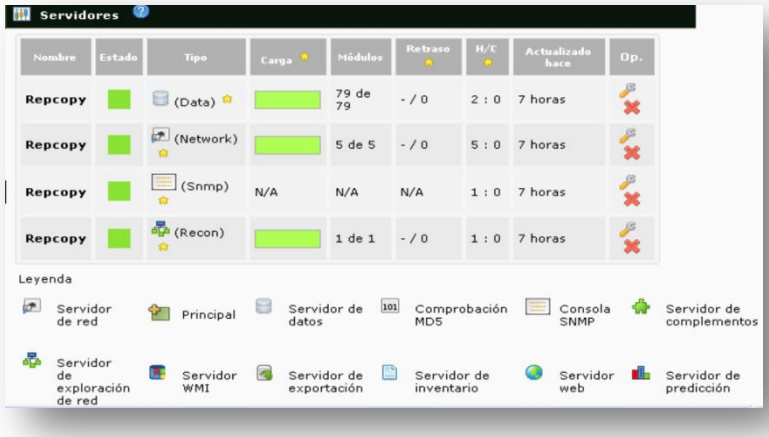
De izquierda a derecha, y de arriba abajo, la cabecera proporciona:

- Información acerca del usuario que está conectado, un enlace directo a su página de usuario (entre corchetes) y el botón de cerrar la sesión.
- Enlace al estado de los sistemas, que muestra el estado de los servidores de Pandora FMS.
- El botón de auto refresco que, además de actualizar la pantalla, puede configurarse para que auto refresque en un intervalo de tiempo seleccionable. Esto permite que en cualquier página pueda definir que esta se refresque cada cierto tiempo, haciendo que no se pierda la sesión y que muestre los datos actualizados.
- La barra de búsqueda que permite buscar en diversos elementos: agentes, informes, alertas, mapas, gráficas combinadas y/o usuarios en la base de datos de Pandora FMS.
- El enlace al visor de eventos del sistema.

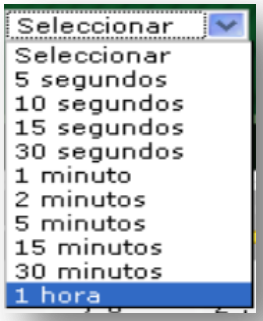
El enlace al estado del sistema avisa también de cuando se cae algún servicio, va cambiando de icono y mostrando cuántos servicios están caídos:



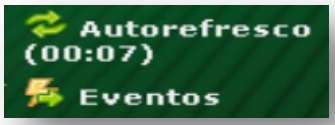
Al pulsar sobre el enlace, éste lleva directamente al estado de los servidores, informando de diversos detalles acerca de los mismos:



El botón de auto refresco permite actualizar la página al pulsar sobre él, o bien seleccionar una frecuencia de actualización:



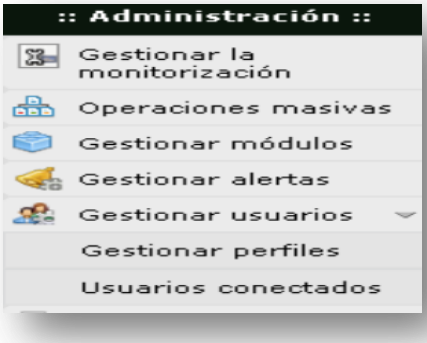
Una vez seleccionada ésta, se mostrará el tiempo restante hasta la próxima actualización junto al nombre del enlace:



- **Gestión de usuarios de pandora FMS**

Para el manejo de esta herramienta debemos establecer los niveles de usuarios con sus respectivos permisos, es decir establecer reglas y dar los permisos a cada uno de ellos a que tendrán acceso y a que no:

Para crear usuarios debemos ubicarnos en el menú administración.



Seleccionamos Gestionar usuarios y nos aparecen los usuarios ya creados anteriormente y un botón para crear nuevos usuarios, al dar clic en este boton nos aparece la siguiente ventana:

Id usuario: Es el nombre o el identificador del usuario es decir, es el nombre con el que aparecerá el usuario.

Nombre completo: Es el nombre del usuario.

Idioma: Como su nombre lo indica es el idioma en el que se manejara el sistema.

Contraseña: Es loa contraseña establecida para el ingreso al sistema.

Perfil global: Es el nivel del usuario es decir definimos si es administrador, o usuario estándar.

Correo electrónico: Es el correo de cada usuario.

Número de teléfono: es el número de teléfono del usuario.

Una vez llenado toso los datos descritos anteriormente damos clic en crear y nos aparece en la ventana el usuario que hemos creado, el siguiente paso es gestionar perfil para el usuario y para esto damos clic en el icono  y damos clic en el botón crear y nos aparece otra pantalla.

Donde debemos elegir las opciones que el usuario podrá realizar en el sistema y damos clic en añadir y listo es todo el proceso para crear usuarios y perfiles de usuarios.

ANEXO 7: CONFIGURACIÓN DE PANDORA FMS

En esta sección se procederá a dar una explicación de la configuración necesario para realizar el monitoreo de los agentes (equipos), la implementación de los módulos a los agentes, mismos que ayudaran a monitorear los servicios si están funcionando o no, establecer alertas para cada uno de los módulos como sean necesario que nos ayuden a controlar los ataques que han sufrido los servidores.

Lo que se busca con esto es explicar paso a paso todo el proceso que hemos pasado para llegar hasta el objetivo general que es tener un sistema multiagente para la detección de ataques en la red de la Empresa Importadora REPCOPY.

Creación del agente

En primera instancia lo que debemos hacer es poder visualizar cada una de las maquinas en nuestro sistema pandora, para esto debemos crear agentes (maquinas) mismos que permitirán monitorear el estado de la misma y su funcionamiento.

Como la base de toda la Empresa gira en torno a un servidor explicaremos la monitorización del servidor de la Empresa en este caso un Windows server 2003.

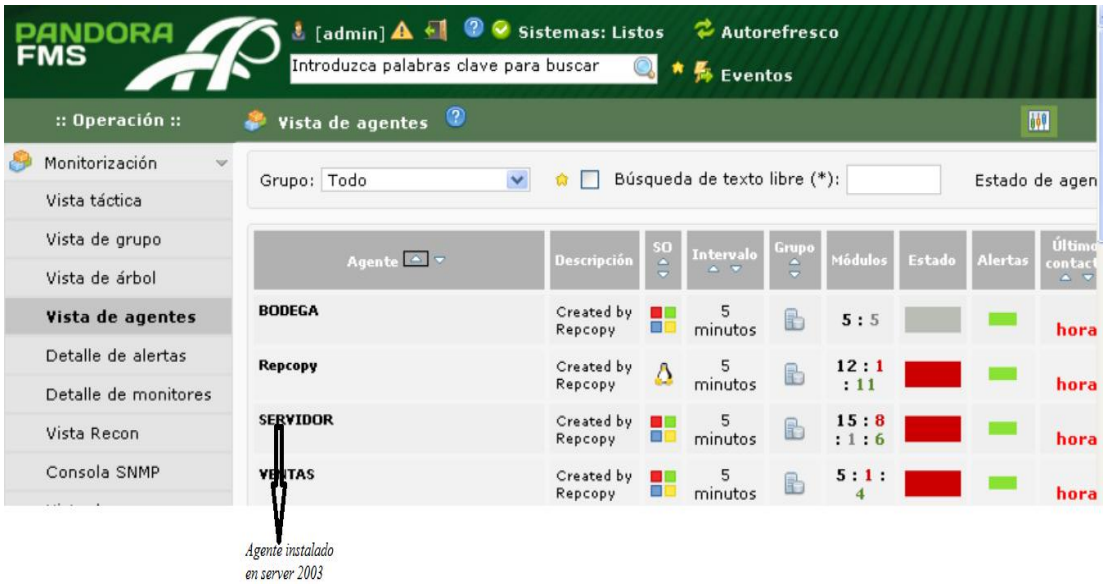
En este caso explicaremos como monitorear equipos con sistemas operativo Windows xp, server.

La creación de agentes se puede realizar de dos formas:

- **Mediante un instalador .exe**

  Para la creación mediante un instalador .exe ver **ANEXO 5:** Instalación del agente windows

  Lo único que debemos hacer en la consola de PANDORA FMS es un refrescamiento o actualizar, una vez hecho esto nos aparecerá el agente con el nombre de la máquina que hemos instalado, para poder ver el agente instalado es dirigirnos al menú operaciones, vista de agentes.



- **Mediante la consola de pandora FMS**

Para esta opción debemos ubicarnos en la consola Web en el **menú administración dar clic en gestionar la monitorización, gestionar agente**

Como podemos ver en la imagen lo único que debemos hacer es dar clic en el botón crear agente donde nos muestra la siguiente imagen:

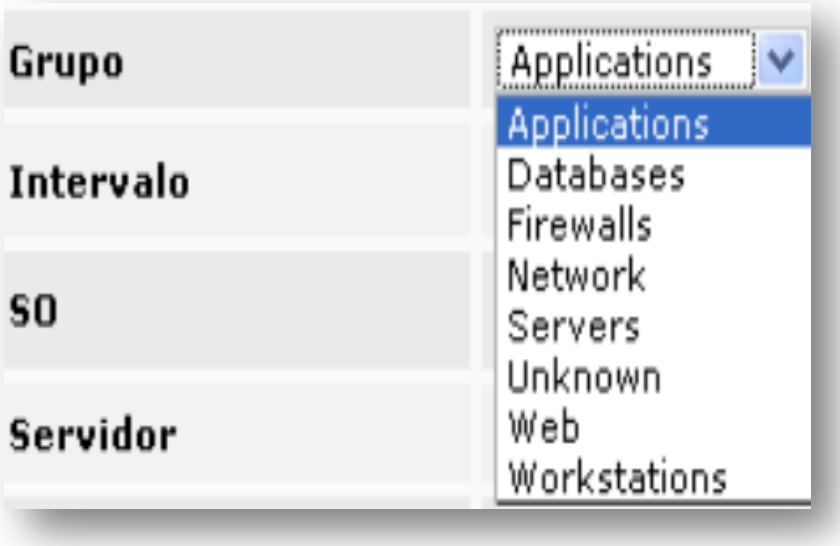
En esta página debemos llenar los campos necesarios para crear el agente que se describen a continuación:

Nombre del agente: Es el nombre con el que se conocerá a la maquina o agente.

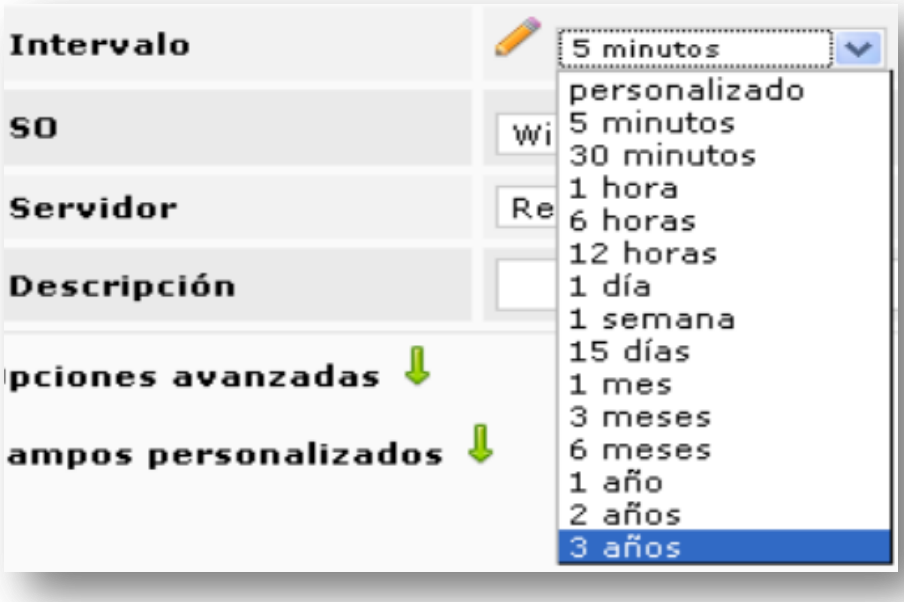
Dirección IP: aquí deberemos poner la ip de la maquina a la que queremos acceder para realizar la monitorización.

Padre: Si queremos que tenga alguna característica de otro agente.

Grupo: debemos escoger a un grupo a la que va a pertenecer el agente las opciones de grupo son:



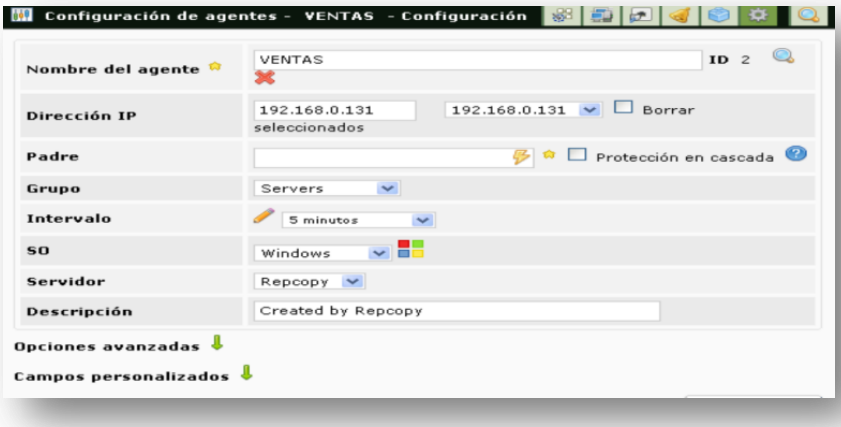
Intervalo: es el tiempo en que queremos que se actualice el agente



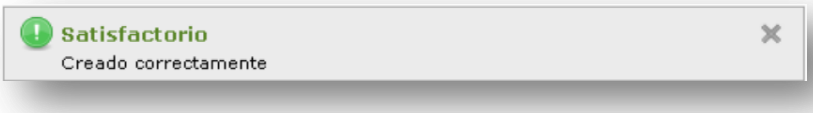
Sistema operativo: Aquí debemos seleccionar el sistema operativo de nuestra máquina.

Servidor: Es el nombre de nuestro servidor pandora a la que estará conectado nuestro agente y donde se guardara información del mismo.
Descripción: Una descripción referente a nuestro agente.

Una vez llenada todos los datos debemos dar clic en crear para que el proceso de creación de agentes esté finalizado.



Y nos aparece el mensaje que nos ratifica la creación del agente.



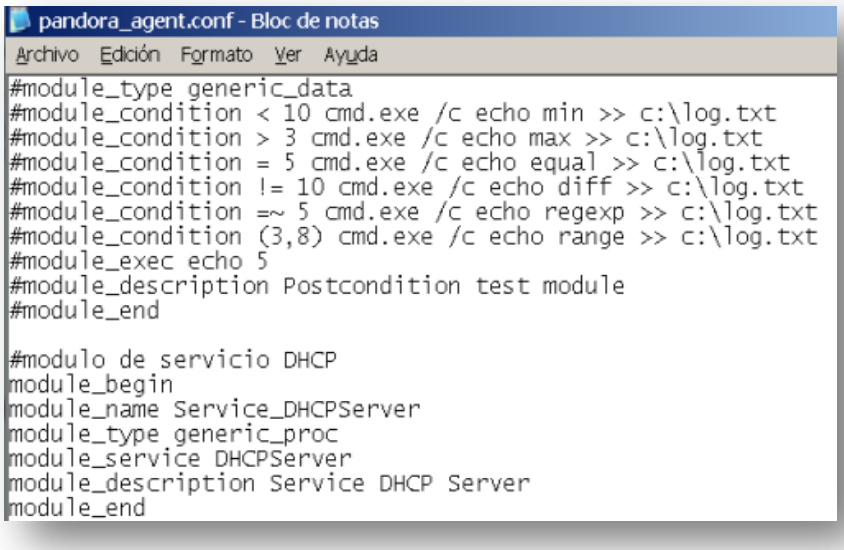
Y para ver el agente creado nos dirigimos al menú operación, monitorización, vista de agente, y en esta página observaremos el agente que hemos creado.

Agregar módulos de monitorización

Una vez creado el agente el siguiente paso es agregar módulos para realizar la monitorización.

Al igual que la creación de agentes se puede hacer de dos formas.

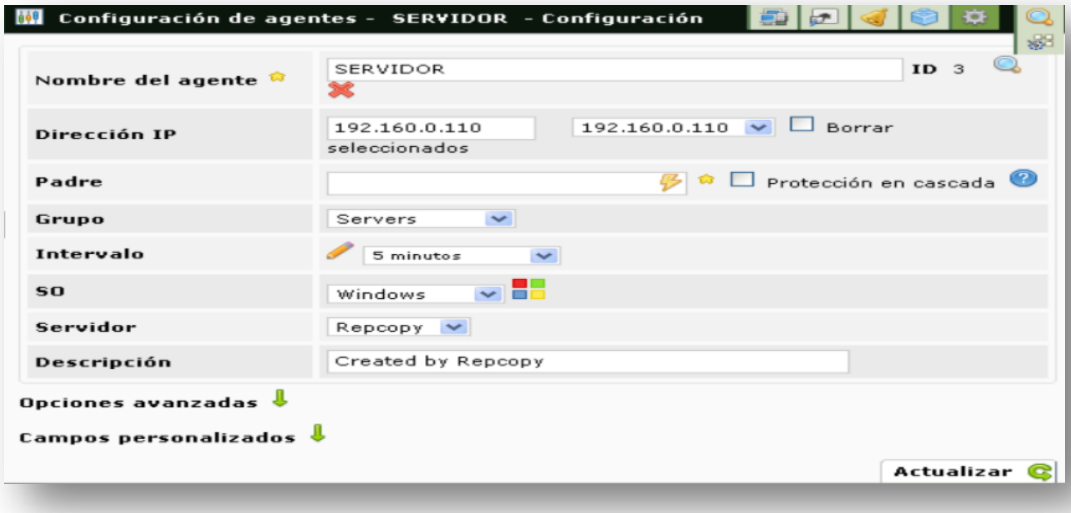
- Mediante el archivo de configuración de pandora que nos aparece al instalar el agente Windows en cada máquina.



Como podemos observar en el archivo de configuración se muestra un ejemplo de un módulo para comprobar el estado del servicio DHCP.

- Mediante la consola Web de pandora, para esto debemos pasar el cursor sobre el nombre del agente y nos aparece tres opciones para realizar operaciones sobre la misma.

Debemos dar clic en la opción editar para poder agregar un módulo, mismo que nos muestra la siguiente imagen.



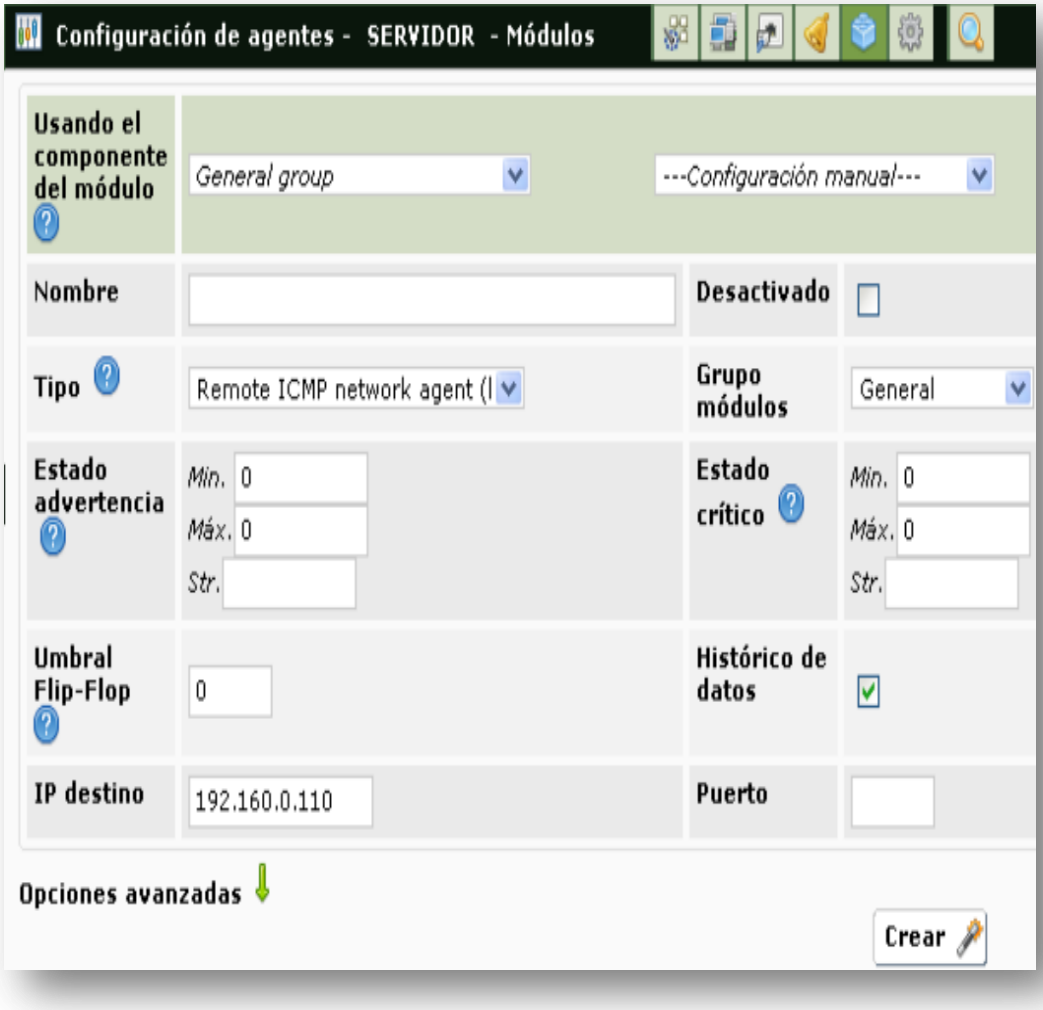
Una vez aquí debemos ubicarnos en el menú de la parte superior izquierda y debemos seleccionar el icono de modulo.

Al dar clic en este icono nos muestra una ventana con los módulos ya creados con la instalación del agente, para agregar un nuevo módulo lo primero que debemos hacer

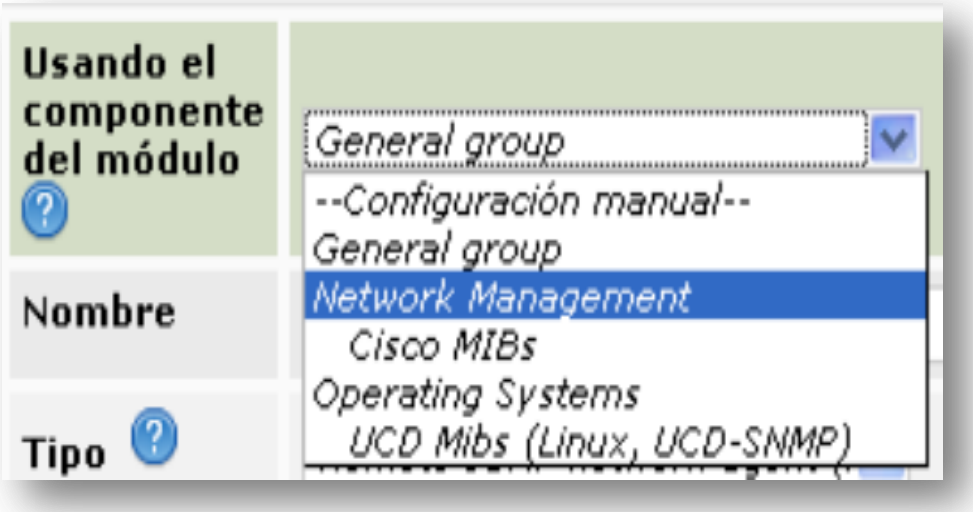
es seleccionar el tipo de modulo que crearemos, para este caso tenemos dos tipos de modulo.

Crear un nuevo módulo de servidor de red.

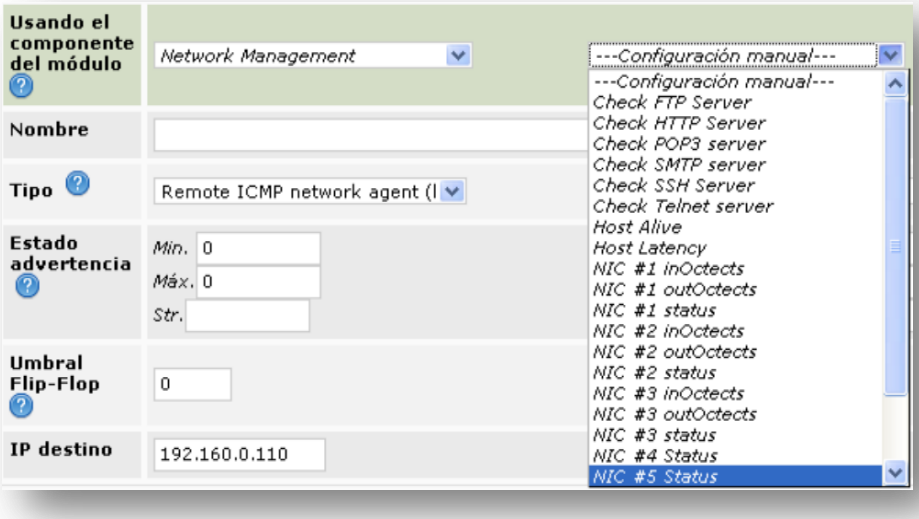
Dependiendo de nuestro caso seleccionaremos un tipo, en este caso seleccionaremos **Crear un nuevo módulo de servidor de red,** y dar clic en el botón crear, y nos aparece la siguiente ventana.



Usando el componente del módulo: debemos seleccionar el tipo de modulo que nos presenta pandora para la monitorización.



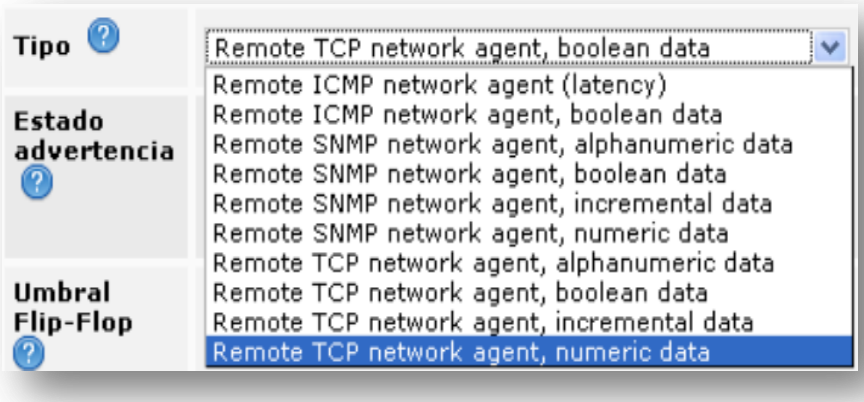
Como podemos observar seleccionaremos **Network Management**



Después seleccionaremos el tipo de chequeo que queremos hacer, como podemos ver en la figura anterior.

Nombre: Es el nombre que le daremos al módulo.

Tipo: En este caso nos da la opción del tipo de monitorización que queremos realizar, aquí debemos seleccionar una a nuestro criterio de monitorización.



Estado de advertencia: Debemos seleccionar un valor mínimo o y máximo para una advertencia

Estado crítico: al igual que el estado de advertencia seleccionaremos un valor máximo y mínimo de estado crítico.

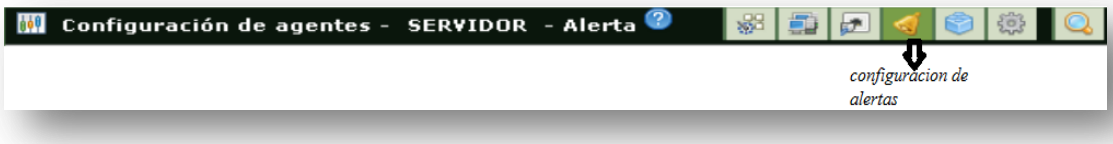
Ip destino: nos aparece ya la ip de la maquina (agente) a la que estamos agregando un módulo.

Una vez llenado todos los datos necesarios debemos dar clic en crear y finalmente veremos nuestro modulo al momento de explorar el agente.

Agregar alertas a cada agente

Otro de los pasos necesarios es agregar alertas para cada módulo creado esto nos ayudara a estar siempre alerta ante las anomalías de nuestro servidor, para esto haremos lo siguiente.

Ubicarnos en el siguiente menú



Damos cli en el icono de la campanita que para nosotros administrador de alertas, el cual nos mostrara la siguiente ventana.

A continuación pasaremos a explicar cada uno de los campos que nos aparecen en la pantalla de alertas:

Modulo: Debemos seleccionar un módulo al que agregaremos la alerta.

Plantilla: Pandora permite seleccionar tres tipos de plantilla que son:

Critical condition: La alerta se disparara cuando el modulo este en estado crítico o el servicio no este iniciado.

Manual alert: La alerta se disparara de forma manual es decir que el administrador del sistema deberá iniciar la alerta.

Warning condition: La alerta se disparara cuando el modulo este en estado de alerta.

Acciones: La plantilla de pandora nos permite adicionar acciones a la alerta, es decir a más de dispararse la alerta se realizara las siguientes acciones:

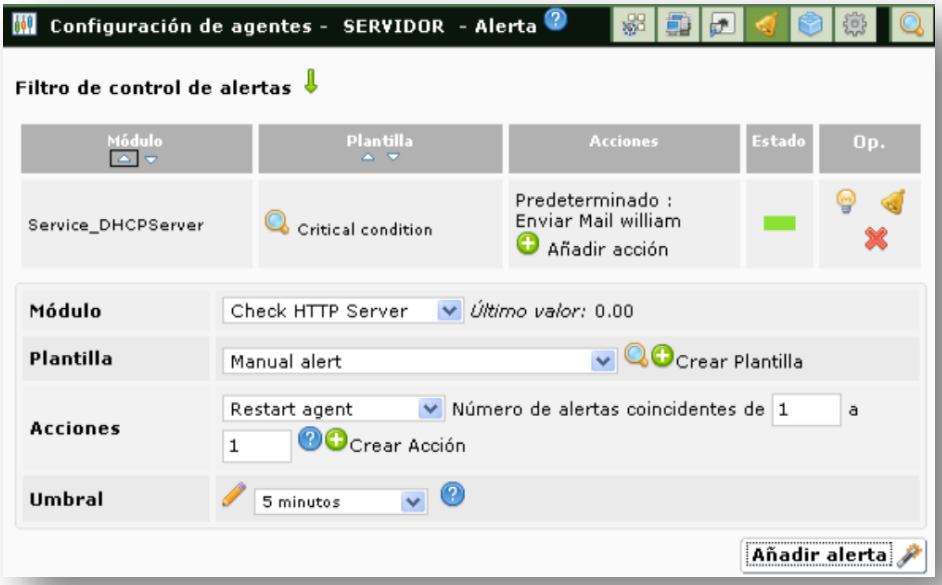
Enviar mail: Al seleccionar la acción de enviar mail, al momento de dispararse la alerta también se enviara un mail al correo electrónico que especificaremos.

Restart Agente: Esta opción permitirá restaurar o reiniciar el modulo que este en estado crítico después de disparar la alerta.

Pandora FMS event: Permitirá adicionar eventos predefinidos por el Servidor Pandora.

Umbral: Aquí definiremos el tiempo en el que queremos que se actualice la alerta:

Una vez llenados todos los campos necesarios damos clic en el botón de añadir alertas:



Una vez dado el clic en el botón añadir alerta nos aparece la alerta que hemos creado, como podemos ver hemos creado la alerta en el módulo chequear el servidor HTTP la alerta será de forma manual.