UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

**Visión Electrónica**

*Más que un estado sólido*

http: revistas.udistrital.edu.co/ojs/index.php/visele/index

VISIÓN ELECTRÓNICA

VISIÓN DE CASO

# Asturiux: sistema de detección de anomalías computacionales

## *Asturiux: detection system of computational anomalies*

***Felipe A. Corredor Ch.***[a]***, Juan D. Villamarín V.***[b]

INFORMACIÓN DEL ARTÍCULO

**Historia del artículo:**
Enviado: Julio de 2014
Recibido: Agosto de 2014
Aceptado: Marzo de 2015

**Palabras clave:**
Anomalías computacionales
Monitorización de eventos
Alertas
Detección
Sistema distribuido
Inteligencia computacional

RESUMEN

En la cotidianidad de la gestión de la red, es complejo correlacionar eventos en diferentes dimensiones: violación legal, intrusiones, fallas por monitorización, violación a políticas de seguridad o incumplimiento de estándares; situaciones a las que se enfrentan profesionales, docentes y estudiantes de esta área en Colombia. Este artículo presenta los aspectos tecnológicos de diseño y desarrollo de un sistema distribuido de detección de anomalías computacionales, denominado "Asturiux", el cual surge de un proyecto de investigación en el área de teleinformática. La problemática se aborda con administración de seguridad en redes y detección de anomalías. El sistema se desarrolla totalmente con software libre, integrando diferentes tecnologías para comunicación, autenticación, persistencia, inteligencia computacional y alertas remotas. Los instrumentos de verificación y pruebas realizadas reflejan un alto grado de eficiencia del sistema, y buena aceptación por los actores implicados.



**Keywords:**
Computational anomalies
Events monitoring
Alert
Detection
Distributed system
Computational intelligence

ABSTRACT

Everyday in network management, it is complex the process to correlate events in different dimensions: legal violation, intrusions, monitoring failures, violation to security policies or breach of standards; to which face professionals, teaching and students in this area in Colombia. This article presents the technological aspects for the design and development of a distributed system for the computational anomalies detection that was termed "Asturiux", which arises as a product from a research project in the teleinformatics area. To addressing this problematic it use the network security administration, and anomalies detection. The system was fully developed with free software, in which were integrated different technologies for the communication, authentication, persistence, computational intelligence and remote alerts. The verification instruments and the realized tests, reflect a high level of system efficiency, and acceptation from the actors involved.

[a]Ingeniero de Sistemas, Magister en Software Libre, Especialista en Diseño y construcción de soluciones telemáticas. Docente de Planta, Universidad de los Llanos. e-mail: felcorredor@unillanos.edu.co

[b]Estudiante X semestre Ingeniería de Sistemas, Universidad de los Llanos, Participante en Investigación, Grupo de Investigación en Tecnologías Abiertas – GITECX, Universidad de los Llanos. e-mail: jvillamarin@unillanos.edu.co

*Citar este artículo como: F. A. Corredor, J. D. Villamarín, "Asturiux: sistema de detección de anomalías computacionales". Visión Electrónica, algo más que un estado sólido, Vol. 8, No. 2, 95-105, julio-diciembre 2014.*

## 1. Introducción

La gestión de las redes es una tarea compleja por la gran cantidad de aspectos a tener en cuenta, y la responsabilidad que recae sobre el administrador: garantizar no solo la disponibilidad de los servicios en la red, sino su integridad y confidencialidad. Cualquier afectación no contemplada o autorizada por el administrador sobre algún dato, servicio y/o recurso dispuesto en la red, incumplimiento de políticas de uso/seguridad, estándares de gestión adoptados y legislación vigente, es considerado una anomalía y debe ser atendida en el menor tiempo posible.

Los administradores deben enfrentarse al anterior problema, definiendo políticas de uso de equipos y de seguridad informática (SI); apoyándose en la legislación vigente; adoptando estándares internacionales para gestión de Tecnologías Informáticas (TI) y seguridad; estableciendo controles y monitorizando, tanto el tráfico para detectar intrusos, como todos los recursos de los hosts presentes en la red. Esto hace que la toma de decisiones en gestión de redes tenga que involucrar directamente la SI y que a los administradores se les deba brindar una formación que les permita implementar estrategias eficaces, de acuerdo a las circunstancias organizativas. Entonces, para incluir adecuadamente la SI en la gestión de la red, debe reflejarse la legislación vigente, políticas y usuarios, normas/estándares, el entorno específico, los datos y los recursos computacionales.

Por otra parte, aunque se han realizado trabajos en detección de anomalías, detección de intrusiones basada en inferencia, y gestión de políticas de SI, estas han asumido el problema de manera aislada, desarrollando herramientas para cada propósito que son muy eficientes en su actividad específica, pero no suponen un apoyo integral a la labor de gestión de la red y la toma de decisiones.

De acuerdo a lo expuesto, esta investigación, desarrolla una alternativa de solución verificada sobre la problemática planteada: Asturiux v1.0., enfocada como herramienta de laboratorio para la línea de teleinformática en la Universidad de los Llanos (Colombia), y generador de conocimiento avanzado para el diseño y desarrollo de nuevos proyectos y herramientas de seguridad en la misma institución.

El artículo se estructura así: en el apartado 2, se contextualiza el problema; en el apartado 3, se describen los materiales y métodos empleados para sincronizar e interactuar en el intercambio de datos y ejecución del proceso de detección, modelamiento apoyado en instrumentos para información, la caracterización funcional y no funcional de la herramienta, y la arquitectura del sistema, y el protocolo de comunicación; en el apartado 4, el desarrollo e implementación de la herramienta; en el 5 análisis y discusión de resultados; en el 6 conclusiones; y en el 7 se reseña alguna perspectiva de trabajos futuros.

## 2. Contextualización del problema

Cualquier afectación no contemplada por el administrador sobre cualquiera de los datos, servicios y/o recursos dispuestos en la red, es una anomalía y debe ser atendida en el menor tiempo posible. Estas pueden ser generadas por un acceso intrusivo, pero también por algún aspecto tecnológico propio de los servicios de la red o los dispositivos (Daño en un disco duro de un servidor, tarjeta de red, dispositivos de interconexión, bloqueo de un sistema operativo, desbordamiento de memoria, sobrecarga del procesador, etc.), por lo que, de acuerdo a la literatura, se puede indicar que "Una de las funciones más importantes del administrador del sistema es que todo funcione de forma segura". Para lograr este propósito, los administradores deberían enfrentarse al problema definiendo políticas de uso de equipos y de seguridad, apoyándose en la legislación vigente, adoptando estándares internacionales para la gestión de TI y seguridad, estableciendo controles y monitorizando no solo el tráfico de la red para detectar intrusos sino todos los recursos de la red (hardware, software y el comportamiento de los usuarios). El problema radica en que el desarrollo de herramientas se ha concentrado en monitorización, detección de intrusos y adopción de estándares; pero cada uno haciendo su propósito de forma aislada, omitiendo además para sus motores de detección, los aspectos relativos al control de políticas de seguridad y la legislación vigente. Este último aspecto es complejo porque la legislación difiere en cada país.

Colombia ha venido fortaleciendo su marco jurídico en aspectos tecnológicos y de seguridad informática a través de: Ley 527 de 1999 - Ley de Comercio Electrónico, Ley 1581 de 2012 - Ley estatutaria de protección de datos personales., Ley 1341 de 2009 - Sociedad de la información y las TICS , Ley 1273 de 2009 - Protección de la información y de los datos, Resolución de la CRC 2258 de 2009 - Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones y el documento CONPES 3701 de 2011 - Lineamientos de Política para Ciberseguridad. En congruencia con lo anterior, los diferentes organismos de estandarización han generado elementos de apoyo a través de estándares como ISO 27000, COBIT, ITIL, OSSTMM entre otros. Pero a pesar de ello, la cantidad de delitos Informáticos aumentó en 67,23% al alcanzar un total de 985 [1]. Por su parte, el reporte global de fraude evidenció que "se revela un problema grave que podría empeorar... el 94% de las empresas colombianas ha sufrido algún tipo de fraude en el último año, frente al 88% a nivel mundial", siendo el

segundo país del mundo (después de China – 98%), y "El 21% de las empresas informaron sobre el robo, ataque en el área de TI" (China reporta el 25% en esta área). Correlacionando, se puede afirmar que, de todos los casos de fraude en Colombia, el 19,7% son realizados a través de las redes de datos y sistemas computacionales [2].

"La monitorización de sistemas es la encargada de supervisar continuamente los diferentes recursos y servicios de la empresa para garantizar el nivel de disponibilidad requerido y en caso de un posible fallo alertar a los administradores para que lo solucionen" [3]. Es decir, la toma de decisiones en administración de redes debe involucrar directamente la SI, y a los administradores se les debe brindar una formación que les permita implementar medidas eficaces de seguridad de acuerdo a las circunstancias organizativas [3], es por ello que para incluir adecuadamente la SI en la gestión de la red, debe reflejarse la legislación existente, políticas, normas, el entorno específico, los datos y las computadoras.

Aunque se han realizado trabajos que abordan la detección de anomalías [5], [6], [7]; detección de intrusiones basada en inferencia [8], [9], [10]; gestión de políticas de seguridad [11], [12], [13]; estas lo han hecho desde su campo específico, sin relacionarse con las demás áreas, dejando un vacío en los requerimientos reales de contexto donde Colombia presenta una situación crítica.

De igual manera, existen herramientas en el contexto como Nagios, Snort y Munin, Pandora FMS©, Cisco Secure©, PRTG Network Monitor©, Pandora FMS©, Zabbix©. El problema de estas soluciones es que son genéricas, en otro idioma y contexto; algunas no realizan alertas remotas, por lo que no correlacionan las dimensiones citadas anteriormente. Por tal razón la detección de anomalías debe estar soportada por herramientas tecnológicas con un buen mecanismo de inferencia de alto nivel de precisión y capacidad de alertar remotamente.

## 3. Metodología

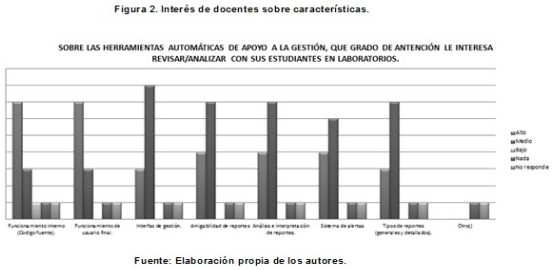
El proceso para definir el modelo, se apoyó en el conocimiento experto existente en las áreas de seguridad en redes e inteligencia computacional, lo cual permitió definir una metodología de detección de anomalías, una arquitectura general, arquitectura de seguridad y mecanismo de inferencia adecuado.

Se aplicaron de manera presencial, y virtual (por email y el sistema surveymonkey®) tres tipos de instrumentos de levantamiento de información a los actores implicados en la problemática (treinta docentes y profesionales del área de teleinformática en la ciudad de Villavicencio) indagando 12 y 16 preguntas en cada caso. Respecto a las características funcionales y no funcionales que se esperan en este tipo de herramientas, los resultados se reflejan en las figuras 1 y 2. Para el caso del primero, es importante resaltar que el 86,6% de los profesionales mostraron un mayor interés por la precisión de detección, la calidad en los reportes, así como en la velocidad del sistema. De otra parte, los docentes del área de teleinformática demostraron una marcada preferencia por el funcionamiento interno y de Usuario final, donde el 53,8% tienen alto interés y 23% interés medio.

**Figura 1.** Aspectos relevantes para Profesionales de Teleinformática.


**Fuente:** elaboracion propia.

**Figura 2.** Interés de docentes sobre características.




**Fuente:** elaboracion propia.

Durante esta fase se diseñó una secuencia metodológica para el sistema, en la cual el servidor y los Hosts sensores se sincronizan e interactúan para intercambio de datos y ejecución del proceso de detección, el cual va desde el lanzamiento del servidor, hasta el envío de la alerta remota por la detección de la anomalía. Esto se refleja en la tabla 1, descriptora del proceso (Servidor [S] y Cliente [C]).

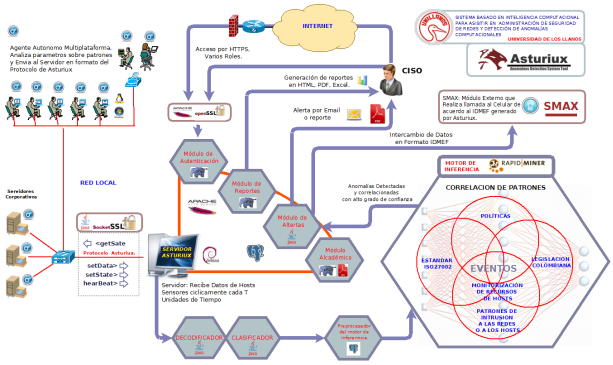
En esta fase se decidió asignar al software el nombre de **Asturiux (Anomalies Detection System Tool)**, para lo cual se definió una arquitectura distribuida y modular (Ver figura 3), en la cual interactúan los actores y módulos del sistema, acorde a la metodología definida previamente. El CISO (Chief Information Security Officer) o Administrador de Seguridad dispone de una interfaz Web (Servidor Apache y PHP), basada en SSL, que le permite acceder a los módulos de reportes, alertas, académico e inteligencia, luego de superar un módulo de autenticación.

**Tabla 1.** Metodología diseñada para Detección.

| EST. | SERVIDOR | CLIENTE | ACCION/ESTADO |
|---|---|---|---|
| 1. | X | | [S] iniciar el servidor de Asturiux, carga configuración de la base de datos BD. |
| 2. | X | | [S] abre el puerto en canal seguro basado en SSL y queda en espera de Clientes. |
| 3. | | X | [C] iniciar el cliente, carga llaves y establece canal cifrado. |
| 4. | | X | [C] El cliente carga la configuración de comunicación de un archivo xml (ip, puerto). |
| 5. | | X | [C] realiza registro, envía comando <getDeviceInfo> (sist. operativo, mac, ip). |
| 6. | X | | [S] genera un barrido y envía comando <getState> a los clientes |
| 7. | | X | [C] verifica hash de xml de configuración de agentes. |
| 8. | | X | [C] carga y ejecuta agentes analizadores de eventos según xml. |
| 9. | | X | [C] recoge resultado de analizadores y codifica datos para envío |
| 10. | | X | [C] Envía comando <setState> (evento:valor...). |
| 11. | X | | [S] Recibe datos y decodifica comando <setState>. |
| 12. | X | | [S] registra estado de las maquinas en la bd. |
| 13. | X | | [S] activa el preprocesador y los registra en tablas dinámicas de la BD. |
| 14. | X | | [S] Lanza el motor de inteligencia computacional (Neural net), modelo basado en Rapidminer. |
| 15. | X | | [S] registra anomalías inferidas en las tablas históricas. |
| 16. | X | | [S] genera estructura IDMEF y la exporta. (Un sistema avanzado de alertas). |
| 17. | X | | [S] activa módulo de alertas y realiza envío de Email. |
| 18. | X | | [S] Genera reporte (formatos web, pdf, excel). |
| 19. | | | Vuelve al estado No. 6. |

**Fuente:** elaboración propia.

**Figura 3.** Modelo Arquitectónico del Sistema de detección de Anomalías Computacionales.




**Fuente:** elaboracion propia.

El resto del sistema (Servidor Asturiux y Host Sensores) está basado en componentes desarrollados en JAVA y Postgres, donde una vez iniciado el servidor, este ordena a los hosts sensores (a través de un protocolo propio) capturar el estado de los hosts y reportárselo. Posteriormente decodifica los datos de todos los hosts de la red y los organiza (pre-procesa) para insertarlos en una red neuronal artificial, la cual actúa como motor de inferencia, determinando la presencia de anomalías en cada host.

En caso de detectarse la anomalía, se genera una alerta y es reportada por varios caminos: envío de correo electrónico al CISO, generación de Reporte en PDF y Excel, registro en Archivo XML formato IDMEF (Intrusion Detection Message Exchange Format) [14]. Este último aspecto, permite la integración de Asturiux con un sistema externo, basado en Asterisk y un modem GSM, para realizar una llamada al teléfono celular del CISO.

### *3.1. Protocolo*

El protocolo de comunicación de Asturiux es un mecanismo de señalización de estados basado en tags y contenido del tipo "¡comando¿ parameter:value; parameter:value;. . . ¡/comando¿". La tabla 2 describe cada comando definido para el protocolo de comunicación propio:

**Tabla 2.** Descripción de comandos del protocolo.

| SENTIDO | COMANDO | DESCRIPCIÓN |
|---|---|---|
| Cliente a Servidor | <getDeviceInfo> | Comando para envío de datos de identificación de la máquina para su registro. <getDeviceInfo> name=linuxfelipe; ip=172.16.6.124; os=Linux; mac=8:0:27:ec:a7:d3; </getDeviceInfo> |
| Servidor a Cliente | <getState> | El servidor solicita información de estado/eventos a los clientes. |
| Cliente a Servidor | <setState> | El cliente envía los datos de eventos detectados al servidor. <setState> 1=0; 2=1; 3=1; 4=1; 5=1; 6=1; 7=1; 8=128; 9=1; 10=1; 11=1; 12=1; 13=1; 14=1; 15=1; 16=1; 17=1; 18=1; 19=1; 20=1; 21=1; 22=1; 23=1; 24=1; 25=1; 26=1; 27=1; </setState> |
| Cliente a Servidor | <heartBeat> | Latido de corazón del cliente al servidor para indicar supervivencia, IDMEF Estructura "idAgent:value;" |

**Fuente:** elaboración propia.

## 4. Desarrollo e Implementación

Para el desarrollo del proyecto se definieron 6 módulos funcionales (ver tabla 3), que interactúan acorde a la arquitectura definida en la figura 3 y el proceso metodológico de la tabla 1. Cada módulo está organiza-

do para consultarlo y/o parametrizarlo desde la interfaz web o archivos XML. (Disponible en http://gitecx.unillanos.edu.co, Opción Proyectos Realizados).

Las herramientas tecnológicas usadas corresponden a Lenguajes de programación, librerías, entornos de desarrollo, servidores web y base de datos, mecanismos de seguridad, herramientas de modelado, entre otras, las cuales fueron seleccionadas acorde a los requerimientos definidos en fases anteriores y cuyo licenciamiento es software libre. A continuación se presenta la tabla 4, del software usado y su aplicación en el proyecto:

**Tabla 3.** Descripción de Módulos.

| ID | MÓDULO | DESCRIPCIÓN |
|---|---|---|
| 1 | Autenticación | Inicio de sesión. |
| 2 | Comunicación | Parámetros de comunicación y tiempos entre barridos. |
| 4 | Alertas | Tipos de Alertas y parámetros de comportamiento y envío |
| 5 | Reportes | Generación y configuración de reportes |
| 3 | Inteligencia | Comandos y parámetros del motor de inferencia. |
| 6 | Académico | Tutor y guía de laboratorio. |

**Fuente:** elaboración propia.

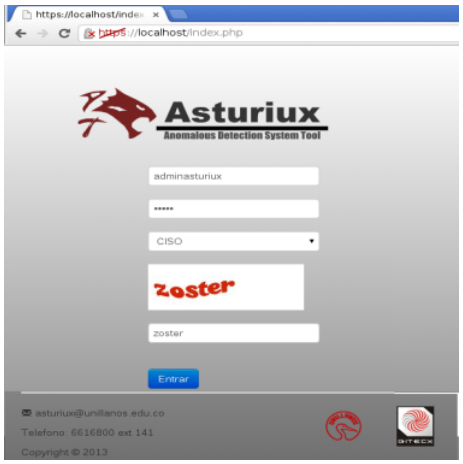
**Tabla 4.** Software usado y descripción de aplicación en Asturiux.

| MÓDULO/ COMPONENTE | HERRAMIENTA TECNOLÓGICA | LICENCIA | TIPO | DESCRIPCIÓN DE USO |
|---|---|---|---|---|
| Comunicación | Java - JDK 1.7 | JRL | Lenguaje de Programación | Entorno en el que se desarrolló tanto el cliente como el servidor. |
| Comunicación | keytool | GNU | Utilidad Java | Generación de claves para uso de sockets protegidos con SSL. |
| Comunicación | OpenSSL | BSD | Protocolo | Capa de seguridad aplicada a los sockets para protección de intercambio de información. |
| Sistema de Administrador | cool-php-captcha | GNU GPL v3 | Librería en PHP | Generación de captcha para protección contra robots que intenten descifrar claves a fuerza bruta |
| Inferencia | rapidminner | AGPL | Librería Java | Motor para inteligencia computacional |
| Inferencia/ Administrador | Postgresql | PostgreSQL License | Motor de base de datos | Gestor de bases de datos usado tanto para el administrador como para el servidor y el cliente. |
| Servidor/ Comunicación | Debian GNU/Linux Squeeze | GNU/GPL | Sistema Operativo | Sistema operativo sobre el cual corre el servidor |
| Servidor/ Administrador | Apache web server | ASF | Servidor Web | Servidor web para servir el administrador del proyecto |
| Administrador | php5 | GNU/GPL | Modulo Interprete PHP | Lenguaje de programación web, con el cual se desarrolló el sistema administrador |
| Todos | Eclipse IDE, 4.2 Juno | EPL | IDE, Software de desarrollo | Entorno integrado de desarrollo, mediante el cual se desarrolló el servidor y el cliente. |
| Modelado | Er-master | BSD | Plugin - Eclipse | |
| Modelado | starUML | GNU/GPL | Aplicación de Software | Generación de diagramas de caso de uso y secuencias, basados en UML |
| Administrador | php-gd | BSD | Librería PHP | Usada para la generación de gráficos para los reportes de las anomalías. |
| Administrador | php-char | GNU/GPL | Librería PHP | Usada para la generación de gráficos para los reportes de las anomalías. |
| Todos | git | GNU/GPL v2 | Sistema de versiones. | Usado para el control de las diferentes versiones y cambios que se le fueron haciendo al proyecto. |
| Alertas | Java-Mail | GPL 2.0 –– CDDL 1.0 | Librería Java | Envío de alerta por email, en formato HTML. |
| Hosts Sensores | JPCAP | MPL 1.1 | Librería Java | Captura de tráfico de red por los hosts sensores |

**Fuente:** elaboración propia.

La interfaz de administración web de Asturiux v1.0, presenta un mecanismo de autenticación fuerte, basado en roles, certificados digitales, funciones hash en passwords y captcha, ver figura 4.

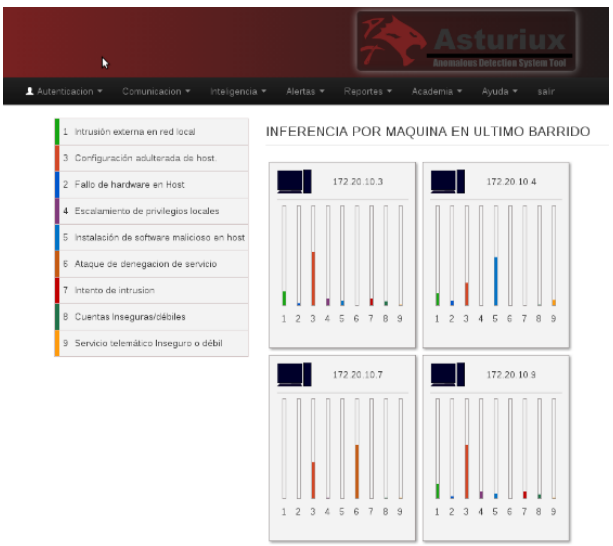
**Figura 4.** Módulo de Autenticación Asturiux.




**Fuente:** elaboracion propia.

Una vez se validan las credenciales de acceso, se dispone de un menú de opciones relacionadas con los módulos del sistema (Autenticación, Comunicación, Inteligencia, Alertas, reportes, académico y Ayuda). En la pantalla inicial se presenta un reporte gráfico, resumen del último proceso de detección realizado, el cual muestra de una manera práctica las anomalías detectadas por cada host de la red, ver figura 5.

**Figura 5.** Reporte inicial interfaz Web.




**Fuente:** elaboracion propia.

Finalmente, Asturiux v1.0 fue sometido a pruebas de funcionamiento y realización de talleres con estudiantes de quinto a décimo semestre del programa de ingeniería de sistemas de la Universidad de los Llanos, sobre una muestra poblacional de 10,1% (26 estudiantes de 257), en los cursos de sistemas operativos y telecomunicaciones III.

**Tabla 5.** Proporción Población estudiantil.

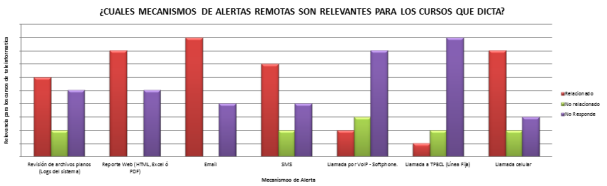
| Semestres | I-IV | IV-VII | VIII-X |
|---|---|---|---|
| Estudiantes | 4% | 58% | 38% |

**Fuente:** elaboración propia.

### Reporte de alertas

Cuando el motor de inteligencia computacional detecta la anomalía, el módulo de alertas realiza el respectivo envío. Para este aspecto, los docentes del área manifestaron una preferencia por el reporte vía Email, ver figura 6. como segundo aspecto se presenta una igualdad en reportes web/pdf y llamada a celular, por lo que se implementaron también estos mecanismos en el sistema (la llamada celular es una integración con un módulo externo desarrollado previamente e integrado a través de IDMEF).

**Figura 6.** Mecanismos de alertas relevantes.




**Fuente:** elaboracion propia.

A través de la API java Mail, se usó una cuenta de correo creada para Asturiux (asturiux@gmail.com), para enviar de manera inmediata un email con el asunto ATENCION: ANOMALIA DETECTADA, que contiene un completo reporte con tablas y gráficos, que sean intuitivos para su análisis y faciliten la gestión al CISO.

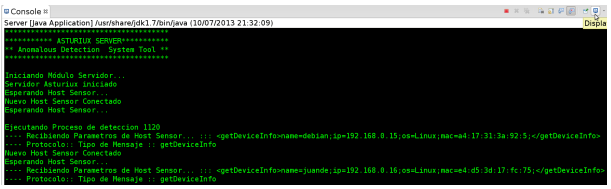
## 5. Análisis y discusión de resultados

La ejecución de Asturiux server, se realizó con varios clientes paralelos en un escenario simulado, donde cada host sensor reporto de manera adecuada sus parámetros de máquina (nombre, dirección ip, sistema operativo y dirección mac). Ver figura 7

Una vez lanzado el servidor, se generaron de manera controlada anomalías que activaron los sensores, como modificación de archivos del sistema, ataques de escaneo de puertos – ver figura 8, (host sensor que lo detecta

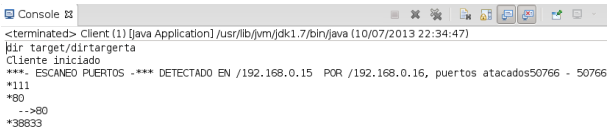
en tiempo real), generación de trafico falso con hping3, detención de servidores, escalamiento de privilegios de usuarios, otros...

**Figura 7.** Servidor Asturiux en Ejecución.




**Fuente:** elaboracion propia.

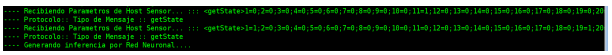
**Figura 8.** Servidor Asturiux en Ejecución.




**Fuente:** elaboracion propia.

Una vez detectado se reciben adecuadamente a través del protocolo, ver figura 9 y son decodificados para su procesamiento (pre-procesador desde java y plsql) antes de ingresar al motor de inferencia (Red neuronal artificial - RNA).

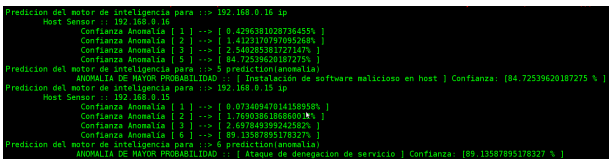
**Figura 9.** Recepción de mensajes de protocolo.




**Fuente:** elaboracion propia.

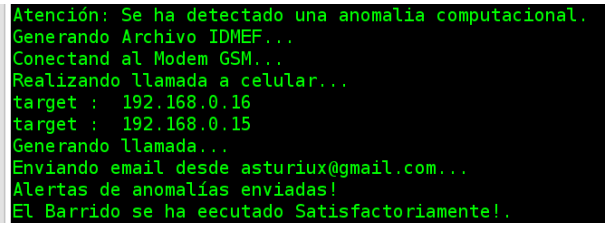
Una vez son analizados por la RNA, se generaron los resultados de confianza por cada anomalía (ver tabla 5), presentándose dos casos particulares, como se observa en la figura 10, lo que permitió determinar que para el 88,8% de los casos detección, el grado de confianza es superior al 83,5%. Esto significa que aplicando un margen de error de 5%, se determinó que el sistema realice acciones de envío de alertas cuando el grado de confianza supere el 79,32%. Ver figura 11.

**Figura 10.** Generación de Resultados por la RNA.




**Fuente:** elaboracion propia.

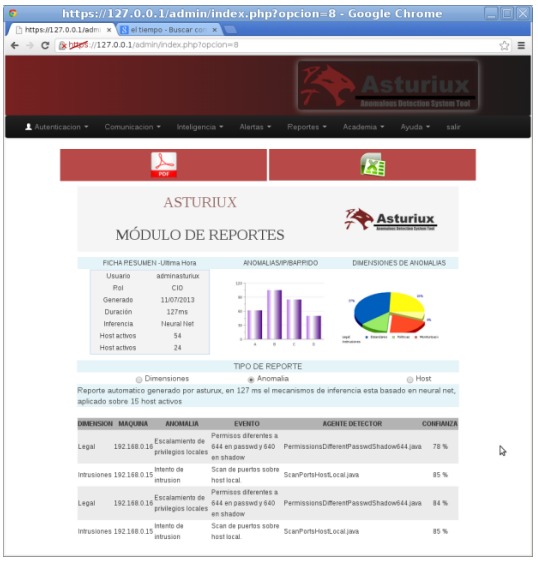
**Figura 11.** Ejecución de alertas remotas.




**Fuente:** elaboracion propia.

El reporte a través de la interfaz web, está disponible en tiempo real al momento de la autenticación y con acciones automáticas de refresco que se realizan cada 2 segundos. Ver figura 12.

**Figura 12.** Reporte HTML/Web de Asturiux.




**Fuente:** elaboracion propia.

Al realizar las pruebas focalizadas por grupo de eventos a cada anomalía; generando la activación de cada uno de los 27 sensores y medidos sus niveles de precisión, se obtuvieron los siguientes resultados:

**Tabla 6.** Resultados de pruebas de precisión.

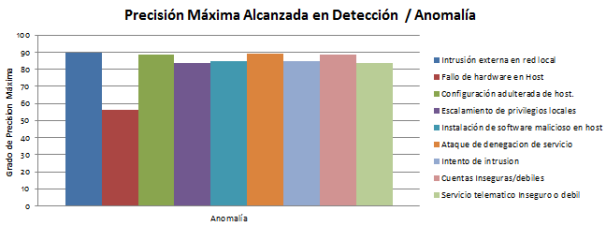
| Anomalía | Precisión | ID Evento | Evento Detectado |
|---|---|---|---|
| Intrusión externa en red local | 89.64% | 1. | Más de una sesión de Usuario root autenticado en el mismo equipo |
| | | | |
| | | 2. | Más de una sesión de Usuario sin privilegio autenticado en el mismo equipo |
| | | 3. | Scan de puertos sobre host local. |
| | | 4. | Apertura de nuevo puerto TCP. |
| | | 5. | Trafico con TTL corto, dirigido a host local desde host externo. |
| Fallo de hardware en Host | 0.5643 | 6. | Sobrecarga de uso de sistema raiz, superior al 80% |
| | | 7. | Sobrecarga de procesador, superior al 80% |
| | | 8. | Sobrecarga de memoria, superior al 80% |
| | | 5. | Trafico con TTL corto, dirigido a host local desde host externo. |
| | | 9. | Host No responde ping |
| Configuración adulterada de host. | 0.8881 | 10. | Archivos de configuración del sistema modificados (iptables, init.d, etc) |
| | | 11. | variable de entorno TMOUT modificada para aumentar el tiempo o nula. |
| | | 7. | Sobrecarga de procesador, superior al 80% |
| | | 8. | Sobrecarga de memoria, superior al 80% |
| Escalamiento de privilegios locales | 0.8397 | 12. | Permisos diferentes a 644 en passwd y 640 en shadow |
| | | | |
| | | 13. | Cambio de propietario y grupo (root, shadow) a shadow |
| | | | |
| | | 14. | Ejecución de su por parte de algún usuario del sistema. |
| Instalación de software malicioso en host | 0.8472 | 15. | Procesos interceptando o ejecutando información de tráfico del tipo keylogger o sniffer. |
| | | 16. | No hay presencia de antivirus en maquina windows |
| | | | |
| | | 4. | Apertura de nuevo puerto TCP. |
| Ataque de denegación de servicio | 0.8913 | 17. | Caída de servicio telemático en puertos estándar (80, 21, 22, 53) |
| | | 6. | Sobrecarga de uso de sistema raiz, superior al 80% |
| | | 7. | Sobrecarga de procesador, superior al 80% |
| | | 8. | Sobrecarga de memoria, superior al 80% |
| Intento de intrusión | 0.8502 | 18. | Numero de fallos de login superior a 3 (auth.log) |
| | | | |
| | | 3. | Scan de puertos sobre host local. |
| Cuentas Inseguras/débiles | 0.885 | 19. | Tiempos de caducidad no administrados en shadow |
| | | 20. | Contraseñas sin cambio hace más de un mes |
| | | | |
| | | 21. | Fechas de caducidad nulas en shadow |
| | | 22. | Cuentas normales (>1000) en passwd sin contraseña |
| Servicio telemático Inseguro o débil | 0.836 | 23. | Servicio ftp con acceso anónimo |
| | | 24. | ftp con acceso anónimo |
| | | 25. | Logs del sistema no se registran. |
| | | | |
| | | 26. | Logs no se están registrando por cada servicio telemático |
| | | 27. | Servicio telemático sin capa de seguridad (no usa certificado digital) |

**Fuente:** elaboración propia.

Después de 1131 procesos de detección y de acuerdo a la tabla 6, se obtiene que el 88,8% de las anomalías se detectan por el motor de inferencia (RNA) con un grado de confianza superior al 83,5%, esto indica un alto grado de precisión en la detección (entre el 80% y 100% es considerado nivel alto, por los expertos en teleinformática), de igual manera las alertas por email tuvieron una tasa de envío exitoso del 98% (Presentándose falla en este último aspecto, por el bloqueo temporal automático de los servidores de Gmail a la cuenta de asturiux@gmail.com, al enviar más de 50 correos similares a la cuenta del CISO durante el mismo día).

La tabla 6, muestra que la "Intrusión externa en red local" es la que presenta mayor precisión 89,65%, ante una activación de los 5 sensores relacionados con sus eventos (A cada evento le fue asignado un peso de incidencia, de acuerdo al conocimiento experto de los profesionales en teleinformática) y la de menor precisión "Fallo de hardware en host" con un nivel medio de 56,4%. A pesar de que estas son dos de las anomalías que más eventos tienen relacionados (5 cada una), esto se debe a que para la anomalía de fallo de hardware, los eventos 6,7 y 8 son los que más se relacionan con otras anomalías y su ocurrencia, reparte porcentualmente la confianza en cada una. Esto obliga a que el proceso de aprendizaje / entrenamiento de la RNA, debe mejorar este resultado a futuro, acorde al desempeño en cada organización donde se instale Asturiux.

**Figura 13.** Niveles de Precisión Máxima.




**Fuente:** elaboracion propia.

Una vez los estudiantes observan el proyecto en funcionamiento con tres talleres diseñados para tal fin, se indaga sobre su percepción ante las características que evidenció en Asturiux, encontrando que la mayoría (92,3%) reconoce que el proyecto generó innovación regional investigativa y que es una herramienta adecuada de laboratorio para el programa de ingeniería de sistemas.

A su vez, Asturiux fue puesto a pruebas y analizado en su funcionamiento con el personal de la policía Nacional de la SIJIN Metropolitana de Villavicencio (jefe de la SIJIN MEVIL, Jefe de delitos informáticos, jefe de telemática, jefe de patrimonio económico y jefe de la unidad antipiratería), quienes observaron y analizaron el funcionamiento de Asturiux, planteando que este sistema es una herramienta muy buena e interesante, que puede impactar positivamente en las empresas de la región, apoyando la seguridad en ellas, principalmente en lo referente a la detección de algunos eventos delictivos contra la ley 1273 de 2009.

**Tabla 7.** Aspectos evidenciados por estudiantes.

| CARACTERISTICAS EVIDENCIADAS EN ASTURIUX, POR ESTUDIANTES | SI | No | No responde |
|---|---|---|---|
| Innovación regional en el campo investigativo de seguridad informática. | 92,3% | 0% | 7,7% |
| Adecuada como herramienta de laboratorio en teleinformática. | 92,3% | 0% | 7,7% |
| Integró alrededor de la investigación, el trabajo de docentes, estudiantes y egresados. | 84,6% | 0% | 15,38% |
| Aplicó y generó de conocimiento avanzado en teleinformática. | 70% | 11% | 19% |

**Fuente:** elaboración propia.

## 6. Conclusiones

- La detección y capacidad de envío de alertas remotas, son dos de los aspectos más importantes para los profesionales del área; Se logró que el 88,8% de las anomalías se detectaran con un grado de confianza superior al 83,5%, y las alertas por email tuvieron una tasa de envío exitoso del 98%. Sin embargo es fundamental disponer al momento de la implantación de este tipo de sistemas basados en aprendizaje, especial atención al proceso de entrenamiento del motor de inferencia.

- Para los docentes del área de teleinformática, la posibilidad de enviar email automáticamente desde un sistema computacional, es el mecanismo que más se relaciona con los cursos en su área, teniendo en cuenta que también la mayoría no solo le interesa revisar el funcionamiento de usuario final sino también el funcionamiento interno de las herramientas que usan y su código fuente.

- Los sistemas de detección generalmente no disponen de mecanismos propios de alertas y reportes; se limitan a registrar en archivos planos, que son tediosos y complejos de analizar y obligan al Administrador de la red a recurrir a la instalación y

configuración de herramientas o módulos externos, que en muchos casos no se integran de la manera adecuada. Los profesionales del sector de teleinformática requieren herramientas de detección y monitorización que no solamente sean precisas y veloces en su detección, sino que sean capaces de enviar alertas remotas en forma oportuna, reconociendo que este es un aspecto fundamental para las herramientas de apoyo a la gestión de la red y que este valor agregado está presente en Asturiux.

- El software libre es un soporte fundamental en procesos de investigación e innovación, ya que se logró demostrar que dispone las tecnologías de calidad y suficiencia para soportar completamente un proyecto de investigación en el campo de la teleinformática, específicamente en seguridad informática.

- El uso de estándares tipo IDMEF, no está muy difundido y por tal razón no son utilizados por los docentes del área de teleinformática; el 100% de los ellos manifestaron en esta investigación, que no aplican formatos de intercambio de datos tipo IDMEF en sus proyectos de investigación y/o desarrollo tecnológicos. En este proyecto se logró implementar eficientemente la integración de dos proyectos del grupo de investigación (Asturiux y SMAX-Sistema para el envío de múltiples alertas remotas ante Incidentes de seguridad informática) que se desarrollaron en paralelo.

- Las herramientas que se desarrollan principalmente en/para otros contextos (países como Estados Unidos y Europeos), presentan limitantes a los CISOS Colombianos, ya que los fabricantes no se interesan por tener en cuenta el marco legal, de igual manera el idioma Inglés sigue siendo una limitante vista por los estudiantes de Ingeniería para la selección y uso de herramientas de detección de anomalías: Para más del 56% de los estudiantes, una herramienta con interfaz y reportes en ingles limita en grado medio y medio alto, las prácticas de laboratorio en estos temas.

## 7. Trabajos Futuros

- Diseñar, implementar e integrar mecanismos de acciones de control y corrección automáticos, acorde a las anomalías detectadas.

- Incorporar nuevos módulos de inteligencia computacional para análisis comparativo de. Precisión. Falsos positivos, falsos negativos, verdaderos positivos, verdaderos negativos.

- Integrar módulos adicionales de detección, basados en hardware y no solo para seguridad lógica sino también para seguridad física.

- Aplicar a otros contextos como la explotación agrícola y pecuaria de la región, la metodología y arquitectura propuesta desde Asturiux, en lo referente a monitorización y detección de anomalías.

## 8. Reconocimientos

Los autores expresan su gratitud a Dios y sus Familias, quienes siempre apoyaron este proceso. De igual manera, a la Universidad de los Llanos por financiar el proyecto y a los Ingenieros José Álvarez y Audel Diaz del Grupo de Investigación GITECX.

## Referencias

[1] Policía Nacional, E. G. Criminalidad y análisis espacial de los delitos en Colombia, 2010. Recup..de http://oasportal.policia.gov.co/imagenes_ponal/dijin/revista_criminalidad/volumen53_1/estudios_estadisticos/cifras.pdf. Mayo 2012.

[2] Kroll Eiu, et ál. Global Fraud report 2011. Recuperado de http://www.krolladvisory.com/media/pdfs/KRL_FraudReport2010-11.pdf. Septiembre 2012.

[3] Villar Eugenio, G. F. Administración avanzada de sistemas informáticos (Primera.). Mexico: Alfaomega-Rama. 2010.

[4] Marks Adam, Y. R. (2008). Information security awareness in higher education: An exploratory study. Computers & Security, 27, 241–253. 2008.

[5] Hoang Xuan Dau, J., & PeterBertok. A programbasedanomaly intrusion detection scheme using multiple detection engines and fuzzy inference. Journal of Network and Computer Applications, 32, 1219–1228. 2009.

[6] Anastasakis Leonidas. The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29, 449–457. 2009.

[7] Clark Andrew J., J. J. D. Data preprocessing for anomaly based network intrusion detection: A review. Computers & Security, 30, 353–375. 2011.

[8] Seredynski Franciszek, P. B. Anomaly detection in TCP/IP networks using immune systems paradigm. Computer Communications, 30, 740–749. 2007.

[9] Yang Ming Su. Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. Expert Systems with Applications, 38, 3492–3498. 2011.

[10] Podgurski Andy, W. M. Application-based anomaly intrusion detection with dynamic information flow analysis. Computers & Security, 27, 176–187. 2008.

[11] Morris Franklin, et ál. Information security policy: An organizational-level process model. Computers & Security, 28, 493–508. 2009.

[12] Goel Sanjay, I. N. Metrics for characterizing the form of security policies. Journal of Strategic Information Systems, 19, 281–295. 2010.

[13] Cuppens Frédéric Cuppens, Y. E. Formal enforcement and management of obligation policies. Data & Knowledge Engineering, 71, 127–147. 2011.

[14] IETF. RFC 4765 - The Intrusion Detection Message Exchange Format (IDMEF). Recuperado de http://www.ietf.org/rfc/rfc4765.txt. Mayo 2012002E