Diseño del sistema de seguridad de la Universidad de Granma.

Design of the security system of the University of Granma.

Manuel José Linares Alvaro, MSc. [1]

Ligia Vanessa Sánchez Parrales, Ing. [2]

Marta Lorena Mendoza Navarrete, MSc. [3]

Kenny Orlando Suasti Alcivar, Ing. [4]

[1]Universidad de Granma, Cuba, Email: cheche@udg.co.cu, mlinaresalvaro@gmail.com, código Orcid: https://orcid.org/0000-0002-1185-7822

[2]Instituto Superior Tecnológico Portoviejo, Ecuador Email: ligia1980@live.com, Código Orcid: https://orcid.org/0000-0002-1719-8944

[3]Universidad Laica "Eloy Alfaro", Ecuador, Email: marthalorenamen1@hotmail.com, Código Orcid: https://orcid.org/0000-0001-9135-5963

[4]Instituto Superior Tecnológico Portoviejo, Ecuador, Email: ksuasti@itsup.edu.ec, Código Orcid: https://orcid.org/0000-0002-0169-920X

Contacto: cheche@udg.co.cu

Resumen

La red de la Universidad de Granma, Bayamo, Cuba, es una de las más grandes de la provincia que lleva su nombre: abarca los trece municipios que la forman, pues sus servidores brindan diversos servicios a cada una de las sedes universitarias (extensiones) que existen en cada región de la provincia. A pesar de que ya lleva 25 años de servicio y funcionamiento, nunca ha existido un hecho que haya comprometido tanto la seguridad de sus sistemas, como la integridad de la información que en sus servidores se almacena, y ello se debe al estricto cumplimiento de las medidas de seguridad y protección establecidas desde un primer momento y sobre todo, al diseño de un robusto sistema de seguridad informática, el cual consiste en la utilización y aplicación de una estrategia combinada de diferentes sub sistemas, que ha ido evolucionando con el transcurso del tiempo y persigue, por una parte, lograr el máximo acercamiento posible del nivel de servicio esperado (SLAs) de la red, a los estándares internacionales (99.9%) y por otra,

garantizar la integridad y la disponibilidad de la información que en los servidores se almacena. Es por ello que este trabajo tiene como objetivo exponer y compartir las acciones que se llevaron a cabo, para implementar el Sistema de Seguridad de la red de la Universidad de Granma, en el cual se realiza un estudio descriptivo de las herramientas de seguridad y gestión existentes y del modo en que el mismo evolucionó y desarrolló.

Palabras clave: seguridad informática, seguridad en redes, gestión de la red, tecnologías de la información, administración de redes.

Abstract

The network of the University of Granma, Bayamo, Cuba, is one of the largest in the province: it covers the thirteen municipalities that make it up, since its servers provide various services to each of the university campuses (extensions) that exist in each province region. Despite the fact that it has been in service and in operation for 25 years, there has never been an event that has compromised both the security of its systems and the integrity of the information stored on its servers, and this is due to strict compliance with the security and protection measures established from the outset and, above all, to the design of a robust computer security system, which consists of the use and application of a combined strategy of different sub-systems, which has evolved over time and seeks, on the one hand, to achieve the maximum possible approximation of the service level expected (SLAs) of the network, to international standards (99.9%) and, on the other, to guarantee the integrity and availability of the information that is stored on the servers. stores. That is why this work aims to expose and share the actions that were carried out to implement the Network Security System of the University of Granma.

Keywords: computer security, network security, network management, information technology, network administration.

Introducción

Actualmente, los procesos y acciones que comprenden el sistema de seguridad de los servidores y estaciones de trabajo de las redes de ordenadores, se hacen cada vez más necesarios y adquieren una nueva relevancia, debido al desarrollo sostenido y exponencial que presentan las tecnologías de la información (TI), lo que ha conducido a un aumento constante de la dependencia de sociedad humana de éstas tecnologías. Con respecto a ello, autores como Marrero y Hernández (2016), señalan que la importancia adquirida por

las tecnologías de la información para el crecimiento y desarrollo de las organizaciones ha impulsado la evolución del concepto de gestión de infraestructuras al concepto de implantación de procesos para la gestión y seguridad de servicios de estas tecnologías. Con respecto a esto, otros autores, son del criterio de que en el mundo actual, las organizaciones dependen cada vez más de las TI, con el propósito de apoyar los procesos que en ellas se desarrollan y cumplir con las necesidades de los clientes, las cuales se hallan en constante cambio y que requieren de una mayor complejidad de los sistemas de información, por ello, los servicios de TI están siendo cada vez más utilizados para apoyar y automatizar las actividades de una organización, con el fin de conseguir aumentar la competitividad de ésta y mejorar su funcionamiento, a través de la generación de valores y la reducción de costes. De esta manera, un correcto funcionamiento de estos servicios es fundamental para la organización y por esta razón, es preciso llevar a cabo una adecuada gestión de los mismos. (Pastor, 2015), y asegurar una correcta organización para garantizar la seguridad y el acceso a la información que en los sistemas se almacena. (Marrero & Hernández, 2016)

Las actuales redes de telecomunicación se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que las componen. Los principales problemas relacionados con la expansión de las redes son la estabilidad de los servicios y la integridad de la información que guardan, así como la accesibilidad a éstos, de ahí la necesidad de un sistema que garantice los aspectos antes mencionados. De hecho se estima que más del 70 % del coste de una red corporativa se atribuye a su gestión, seguridad y operación. Por todo ello, la gestión de redes, como conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación, se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones. (López, 2010; Pérez, 2013; Trujillo Alvira, 2022)

La Universidad de Granma (UdG), es la principal institución de educación superior de la provincia que lleva este mismo nombre y abarca, por medio de sus centros universitarios municipales y unidades docentes, los 13 municipios de la provincia la cual posee una superficie de 8377 km^2.

En la UdG se estudian más de 15 carreras y cuenta actualmente con unos 20 000 estudiantes, su red de ordenadores de la UdG se fundó en diciembre de 1996. Se conectó

a redes públicas en 2003 por lo que fue necesario rediseñar el sistema de seguridad existente hasta el momento y organizar uno que garantizara las nuevas exigencias. Actualmente posee más de 5000 computadoras conectadas la red en todas sus sedes.

Partiendo de lo antes expuesto, puede señalarse como **problema** existente, la necesidad (a partir de 2004) de un sistema de seguridad que garantizara la integridad, preservación y disponibilidad de la información que en los servidores de la red de la Universidad de Granma se almacenaba, así como la estabilidad y disponibilidad de sus servicios.

Esta investigación tuvo como **objetivo**, exponer y compartir las acciones que se llevaron a cabo, para implementar el Sistema de Seguridad de la red de de la Universidad de Granma, así como el modo en que éste ha ido evolucionando y desarrollándose.

Desarrollo

El proceso de implementación del sistema de seguridad de la red de la Universidad de Granma, ha ido perfeccionándose a lo largo de los años hasta convertirse en lo que es hoy; comenzó apartir del momento en el que se instalaron los primeros servidores y servicios que existieron en la red, en aquel entonces solo brindaban los servicios de correo electrónico y almacenamiento de archivos. Esta primera etapa del sistema de seguridad de la red se caracterizaba por el empleo de pocas herramientas aisladas, y los sistemas de seguridad eran prácticamente nulos: se trataba de mantener los sistemas antivirus actualizados, era controlado el espacio de almacenamiento de información por parte de los usuarios, así como los diferentes niveles de accesos a los servidores. Existía un sistema de control de acceso físico a los equipos, y se tomaron medidas para evitar el abuso en los sistemas de correos: tamaño máximo de correos a enviar, tipos de archivos, capacidad de almacenamiento en los buzones y el envío de correos masivos controlados y asignado solo a los usuarios autorizados a ello.

La segunda etapa se inició a partir del momento en que la Universidad de Granma se conectó a redes públicas mediante canales de datos dedicados (2004), lo cual facilitó la conexión de ésta a redes públicas como internet y otras redes externas. En aquel momento, el canal contaba con una velocidad de 64 kbps.

En el momento que se realizó la conexión de los servidores de la entidad a redes públicas, inmediatamente surgieron nuevos servicios tanto locales como remotos: navegación, accesos a bases de datos y materiales académicos, gestión y búsqueda de información,

directorios, automatización de procesos, etc; por lo que pronto fue evidente la necesidad de garantizar, tanto la confidencialidad como la fiabilidad, autenticidad, y accesibilidad a informaciones y servicios, es decir, la necesidad de un sistema de seguridad que garantizara las nuevas exigencias.

A partir del enlace a redes públicas, el proveedor de servicios solo podía asegurar una conexión de datos a través de un solo canal, por lo que la red paso a tener una topología en forma de árbol o jerarquizada. Por ello el elemento inicial en esta segunda etapa de desarrollo del sistema de seguridad fue la creación un Sistema de seguridad capaz de aprovechar las ventajas que esta clase de topología brinda para el filtrado y control de paquetes IP, a través del control de los flujos de información de entrada / salida desde y hacia la red privada.

En sus inicios, la segunda etapa se caracterizó por:

- Existencia de 2 routers en la red (Figura 1).
- Existencia de una red DMZ o zona desmilitarizada para los sistemas que tenían que tener visibilidad desde el exterior con direccionamiento IP público.
- Existía otro segmento de red interno, en el cual las estaciones de trabajo compartían la misma subnet que los servidores.
- No se empleaban protocolos seguros (https, ssl, etc)

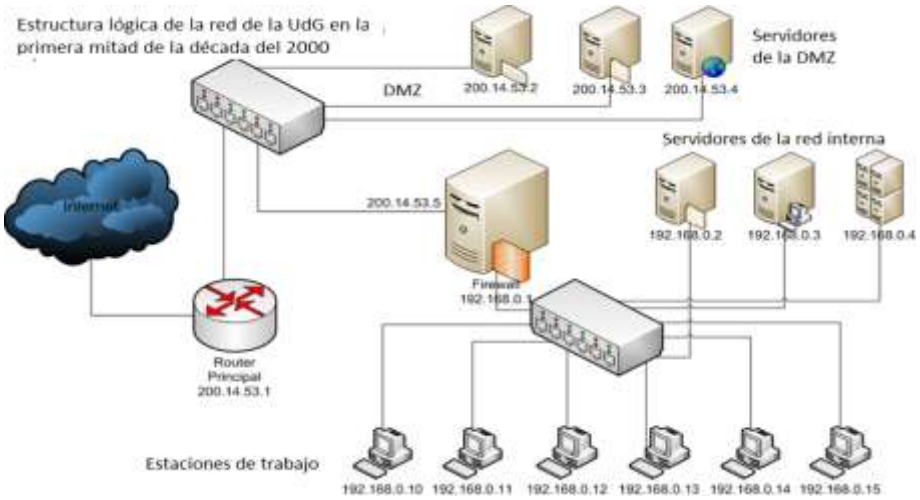

Figura 1. Esquema lógico de la red de la UdG en el período comprendido entre los años 2004 y 2006

En la figura 1 se puede apreciar un esquema que representa la red de la Universidad de Granma a partir del año 2004, puede notarse que no existía un firewall en el router de borde, ni firewalls locales en los servidores de la red de la zona desmilitarizada (DMZ). Otra gran vulnerabilidad era el uso de un mismo segmento de red, tanto para las estaciones de trabajo de la institución como para los servidores internos que almacenaban algún tipo de información sensible.

Precisamente por las vulnerabilidades existentes en la topología antes descrita, a finales de 2005 existieron serios problemas de seguridad: ataques que ocurrieron desde la propia red interna, pues algunos usuarios avanzados, principalmente estudiantes y técnicos informáticos, comenzaron a emplear sniffers para apoderarse de contraseñas de cuentas de usuarios con privilegios especiales.

Esta situación implicó la necesidad de un rediseño topológico en la red y los firewalls, lo cual condicionó el surgimiento de una nueva etapa en el desarrollo de la red a partir de principios de 2006, y entre las acciones más importantes se pueden mencionar:

- La creación de una subred o segmento de red adicional para los servidores internos.
- La creación de varias subredes para las estaciones de trabajo de la LAN del centro, pero que no formaban parte de los servidores interiores.
- Filtrado de paquetes entre todas las subredes, empleando el firewall IPTables.
- Empleo de protocolos seguros con SSL, principalmente HTTPS, sobre todo para cualquier servicio que implicara autenticación a través de la red. (aunque no se contaba con certificados de seguridad válidos)
- En este momento comenzaron también a desarrollarse los sistemas de gestión y monitoreo de la red y resguardos de información como un sistema independiente a los de seguridad.
- En el router de borde se implementó un firewall empleando las instrucciones de Cisco IOS.
- El router – firewall interno se actualizó al Sistema operativo Linux Fedora Core, y el filtrado de paquetes se implementó con IPTables. Se filtraban tanto los datos entrantes para el propio firewall (INPUT) como para el tráfico de tipo FORWARD.

- A cada uno de los servidores, tanto de la DMZ, como de la red interna de servidores (good), se le implementó a su vez un firewall local con IPTables para las cadenas de tráfico entrante (INPUT).

En la figura 2 se puede apreciar la nueva topología que se adoptó a partir de este momento: se segregaron los servidores en una nueva red o segmento, y se implementaron firewalls o cortafuegos independientes para cada servidor, ya fuera interno (red interna) o externo (DMZ).

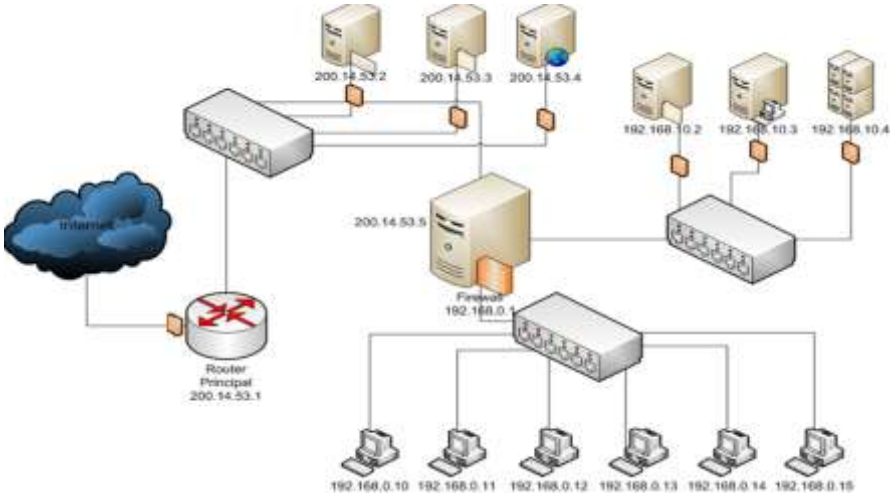

Figura 2. Topología que se desarrolló en la red a partir del año 2006.

A pesar de todo, existían serias limitaciones en los inicios de este segundo período: no existía la forma de acceder a certificados ssl válidos, no existía redundancia en el cableado de la red, y los equipos, ni un robusto sistema de gestión que garantizara la disponibilidad y estabilidad de los servicios. Tampoco se empleaba la virtualización de servidores y servicios.

A partir de 2016, con el proceso de virtualización comenzó a desarrollarse en la red de la UdG, y el establecimiento de sistemas redundantes en los dispositivos y cableado, redes SAN, la subida de la velocidad de conexión y el crecimiento que había tenido la red en los últimos años, era necesario entonces un sistema de seguridad que consistiera en una estrategia combinada de diferentes sub sistemas, y por una parte, que fuera capaz de lograr el máximo acercamiento posible del nivel de de servicio esperado (SLAs) de la red, a los estándares internacionales (99.9%) y por otra, garantizar la integridad y la disponibilidad de la información que en los servidores se almacena; además, debían ser integrador, pues debería incluir sistemas que se habían venido desarrollando de manera independiente,

tales como el sistema de resguardos o copias de seguridad, el sistema de gestión y los sistemas detectores de intrusos y anomalías en la red. (Figura 3)

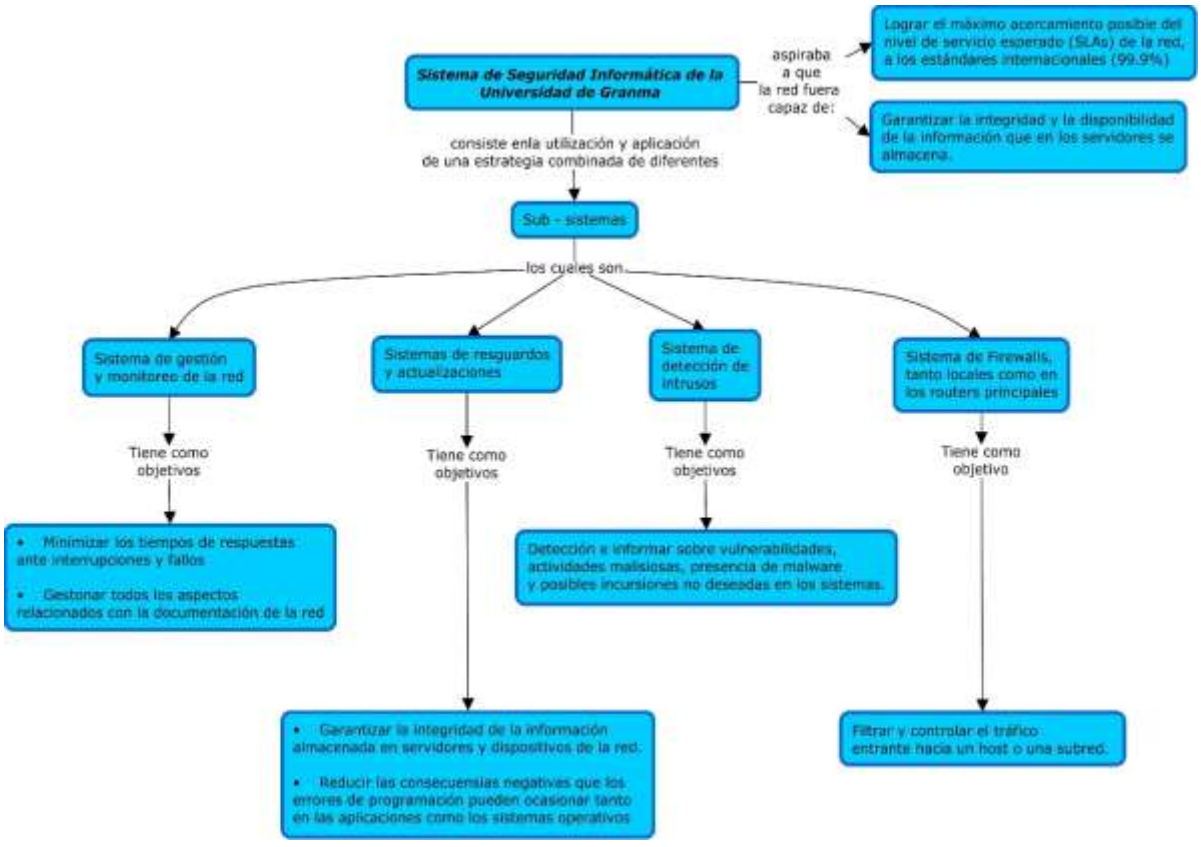

Figura 3. Caracterización del sistema de seguridad informática actual existente en la Universidad de Granma, donde se destacan los subsistemas que lo forman.

Sub sistema de gestión y monitoreo de la red.

El proceso de implementación del sub sistema de gestión de redes de la Universidad de Granma, se caracterizó, a partir de 2016, por organizarce como un sistema e integrador, basado en la aplicación de modelos respaldados por normas internacionales.

Actualmente se conoce la existencia de varios modelos para gestionar una red de ordenadores. Luego de valorar las ventajas, desventajas, complejidad para su implementación y características que ofrecía cada uno de los modelos, se optó por emplear el FCAPS, por sus facilidades para establecer de manera sencilla, rápida y eficiente los diferentes procesos necesarios para implementar un adecuado sistema de gestión de red. Este modelo, constituye uno de los que tiene mayor aceptación y uso. (Gómez & González, 2013). Este modelo a su vez es el recomendado por la ISO (International Organization for Standardization) para la interconexión de sistemas

abiertos, y expresa cinco categorías en las que el modelo divide las funciones de la gestión de redes: fallos, configuración, contabilidad, desempeño y seguridad. (Ding, 2009)

En la implementación del sub sistema de gestión de la red, se tuvieron en cuenta las categorías en que el modelo divide el proceso de gestión y se ubicaron y definieron con claridad las diferentes fuciones y roles en cada una.

Básicamente el sistema de gestión estaba formado por un conjunto de herramientas de software, las cuales se eligieron teniendo en cuenta varios criterios:

- Herramientas basadas Software libre y código abierto, con la finalidad de poder emplearlas dentro de los marcos legales, adaptarlas a las condiciones locales de la red y reducir al máximo los costes de implementación.
- Todas las aplicaciones deberían tener una Interface de de acceso y si fuera posible también de manejo y administración basada en HTML, con el objetivo de facilitar el acceso a la información que suministrasen.
- Preferencia por software diseñado para sistemas operativos de tipo Linux, sin importar su distribucion.

En la tabla 1, se muestran las aplicaciones que han sido seleccionadas y se emplean en este momento, asociadas con la categoría del proceso de gestión de la red de acuerdo al modelo FCAPS, con un resumen de su función o empleo.

Categorías	Software o Aplicación empleado	Función (resumida)
Gestión de la configuración	GLPI	Documentación de la red, gestión de inventarios y activos, etc.
	Bacula	Gestión de los resguardos de las configuraciones
	Nagios	Registros de topología dinámicos
	OCS Inventory	Gestión de Inventarios.
	Rancid	Control de versiones y configuraciones en routers y switchs
Gestión de Fallos	Nagios	Detección de servicios reinicio, notificando el evento.

Gestión de los registros y contabilidad	LightSquid	Herramienta para analizar el acceso a internet por parte de los usuarios de la UdG
	SARG	Similar al anterior.
	SQStat	Herramienta para analizar en tiempo real, el acceso a internet por parte de los usuarios de la UdG
	FreeSA	Similar al LightSquid y SARG.
	Webalizer	Similar al LightSquid, SARG y FreeSA, pero más orientado a resúmenes estadísticos generales que al análisis por usuario.
	Sendmail Analyzer	Análisis del comportamiento del tráfico de correos y todos lo relacionado con éste.
	OCS Inventory	Inventarios de los activos de TI.
Gestión del desempeño	Cacti	Gestión del tráfico y el rendimiento. Brinda una idea rápida del comportamiento del ancho de banda en las diferentes interfaces de los dispositivos de la red, canales de enlaces, interfaces de red en los servidores, etc.
	NFsen+NFsight+SSHCUre	Herramientas similares al NetFlow de Cisco. Determinantes tanto para gestionar desempeño por protocolo de alto nivel, como la seguridad.
	SmokePing	Monitorea los tiempos de retardo de la red y los servicios.
	LibreNMS	Chequeo de la disponibilidad y el hardware de los recursos de la red.
	Nagios	Monitorea la disponibilidad de hardware y servicios.
Gestión de Seguridad	NFsen+NFsight+SSHCUre	Similar al NetFlow de Cisco. Determinantes tanto para gestionar desempeños por protocolos de alto nivel, como la seguridad.
	OSSIM	Sistema de detección de intrusos, eventos de seguridad y vulnerabilidades.
	Bacula	Sistema de resguardos.

	SmokePing	Tiempos de retardo de la red y los servicios.
	Cacti	Comportamiento del ancho de banda en los diferentes routers, canales de enlaces, interfaces de red en los servidores, etc.

Tabla 1. Categorías en el sistema de gestión implementado, asociadas al software que se emplea para su implementación.

Hasta aquí es importante mencionar, que, por su importancia, existen sistemas que por normas, se incluyen dentro del sistema de gestión de la red, pero por su importancia, se decidieron tratar como sub sistemas independientes, tales como el sistema de resguardos y los sistemas de seguridad de la red.

Los procesos de gestión de las configuraciones, fallos y Gestión del desempeño, se realizan empleando Nagios, el cual es una de las principales aplicaciones empleadas en la gestión y chequeo de la red, se trata de una aplicación libre y de código abierto, muy ampliamente utilizada, cuenta con una interfaz web para la monitorización y manejo y chequea tanto servicios de red (SMTP, POP3, HTTP, SNMP, etc) como recursos de hardware en ordenadores o dispositivos (carga del procesador, uso de los discos, memoria, estado de los puertos, etc). Es independiente al sistema operativo, brinda la posibilidad de monitorización remota mediante túneles SSL cifrados o SSH o utilizando el servicio NRPE. La cantidad de plugins existentes es enorme, de hecho, se puede plantear que existen plugins para monitorear casi, cualquier proceso. Ofrece varias maneras de informar la ocurrencia de fallas de servicios o hosts: Otro aspecto importante del Nagios es la posibilidad de restablecer un servicio, después de detectada una falla, e informar al administrador. (Nagios, 2022)

Cuando se proyectó la instalación del Nagios como parte del sistema de gestión, se establecieron parámetros comunes a monitorear en los principales hosts que alojaban servicios en la entidad: espacio disponible los dispositivos de almacenamiento, particiones y archivos de intercambio; carga de trabajo en cada host, uso del procesador, usuarios conectados por SSH, total de procesos en ejecución, estado de la sincronía con los servidores de tiempo de la UdG, etc; y también se definieron parámetros específicos a chequear en función de los servicios que brinda cada servidor o host, por ejemplo, en la figura 4 se muestran los parámetros que se vigilan para un host que hospeda uno de los sistemas de correo entrante: se monitorean, además de los parámetros comunes, el estado

del cliente del sistema de resguardos, el nivel de actualización del antivirus (Clamav), el tamaño de la cola de correos, el estado de procesos propios del sistema de correos como son el sistema antispam, el antivirus y el programa de transporte de correos.

El sistema se diseñó para que emitiera las alarmas se enviaran tanto por el mensajero instantáneo local (OpenFire) como por correo electrónico.

En cada servidor existe un grupo de servicios fundamentales que en caso de que estos se detuvieran por cualquier causa, el Nagios se encarga de intentar ponerlos en funcionamiento nuevamente, por ejemplo, el Squid en el servidor proxy, el Postfix en los servidores de correos o el Apache en los servidores web.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
mail	/ Partition	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	DISK OK - free space: / 17624 MB (92% inode=99%):
	/boot Partition	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	DISK OK - free space: /boot 4515 MB (97% inode=99%):
	/home Partition	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	DISK OK - free space: /home 16845 MB (80% inode=99%):
	/opt Partition	OK	25-07-2016 10:18:57	0d 23h 0m 41s	1/4	DISK OK - free space: / 17624 MB (92% inode=99%):
	/tmp Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /tmp 38068 MB (99% inode=99%):
	/usr/local Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /usr 12799 MB (90% inode=94%):
	/var Partition	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	DISK OK - free space: /var 7820 MB (82% inode=99%):
	/var/log/ Partition	OK	25-07-2016 10:16:22	0d 22h 58m 16s	1/4	DISK OK - free space: /var/log 33159 MB (88% inode=99%):
	/var/spool/amavisd Partition	OK	25-07-2016 10:16:23	0d 22h 58m 16s	1/4	DISK OK - free space: /var/spool/amavisd 17494 MB (92% inode=99%):
	/var/spool/postfix Partition	OK	25-07-2016 10:16:23	0d 22h 58m 15s	1/4	DISK OK - free space: /var/spool/postfix 18946 MB (99% inode=99%):
	Bacula-fd Status	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	PROCS OK: 1 process with command name 'bacula-fd'
	Clamav Update	OK	25-07-2016 10:16:24	0d 22h 58m 14s	1/4	ClamAV OK: daily.cvd 21967 (Mon Jul 25 07:06:06 2016) is up to date
	Current Load	OK	25-07-2016 10:18:57	0d 23h 0m 41s	1/4	OK - load average: 0.03, 0.12, 0.13
	Current Users	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	USERS OK - 0 users currently logged in
	HTTP	OK	25-07-2016 10:17:23	0d 22h 57m 15s	1/4	HTTP OK: HTTP/1.1 200 OK - 259 bytes in 0.003 second response time
	NTP Synchronization	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	Synchronized with the server: 200.14.53.29 offset: -1.045
	Postfix Queue	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	OK: Mail queue is empty
	Running Amavisd	OK	25-07-2016 10:18:58	0d 22h 55m 40s	1/4	PROCS OK: 3 processes with command name 'amavi'
	Running Apolicy	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	PROCS OK: 1 process with command name 'twistd'
	Running Clamd	OK	25-07-2016 10:18:58	0d 23h 0m 40s	1/4	PROCS OK: 1 process with command name 'clamd'
	Running Postfix	OK	25-07-2016 10:18:58	0d 22h 55m 40s	1/4	PROCS OK: 1 process with command name 'master'
	Running Spamassassin	OK	25-07-2016 10:16:23	0d 22h 58m 16s	1/4	PROCS OK: 3 processes with command name 'spamd'
	SMTP	OK	25-07-2016 10:16:22	0d 22h 58m 16s	1/4	SMTP OK - 0.010 sec. response time
	SSH	OK	25-07-2016 10:16:24	0d 22h 58m 15s	1/4	SSH OK - OpenSSH_6.6.1 (protocol 2.0)
	Swap Usage	OK	25-07-2016 10:16:23	0d 22h 58m 15s	1/4	SWAP OK - 100% free (8191 MB out of 8191 MB)
	Total Processes	OK	25-07-2016 10:17:16	0d 22h 57m 22s	1/4	PROCS OK: 190 processes with STATE = RSZDT

Figura 4. Diferentes parámetros chequeados para el host que aloja el sistema de correos entrantes de la UdG.

Sistemas de seguridad y detección de intrusos.

Este se implementó empleando el software Alienvault OSSIM. (Open-Source Security Information Management). En estos momentos se emplea la version 5.8.10 y se actualize diariamente.

Se trata de una colección de software bajo la licencia GPL, agrupadas con el objetivo de ofrecer una herramienta que ayude al manejo de eventos de seguridad mediante un motor

de correlación y una colección detallada de aplicaciones útiles al administrador para tener una vista de todos los aspectos relativos a la seguridad en su infraestructura. OSSIM se ha diseñado para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y vulnerabilidades. Entre las aplicaciones más conocidas que lo forman, podrían mencionarse el Arpwatch, el Pads, para la detección de anomalías en servicios, el Openvas para detectar de intrusos utilizando un escáner de vulnerabilidades, el Snort o Suricata para los eventos de la red, también lo forman otras aplicaciones como el Nessus, NTop, NFSen, entre otros. En estos momentos existe un host en la UdG que aloja el OSSIM, con varios sensores distribuidos en los diferentes campus que de la Universidad de Granma.

Es importante mencionar que en la UdG existe un centro de datos primario, pero también hay sendos centros de datos secundarios en las dos sedes más grandes. El sistema de detección de intrusos se diseñó de manera que existan 3 sensores, uno en cada centro de todos, cuyo sistema primario se encuentra en el centro de datos principal.

Mediante esa herramienta se realizan escaneos de vulnerabilidades semanales empleando OpenVAS, y las vulnerabilidades resultantes son informadas a los responsables directos de cada servidor y sistema, se vigila constantemente todo el tráfico que pasa a través de los routers (eventos de tipo NIDS), generándose alarmas de seguridad cuando se estima que la peligrosidad de un evento pasa determinados parámetros, se analizan los registros de las aplicaciones para la detección de intrusos con ossec-hids, y se generan reportes de seguridad sistemáticos.

En la figura 4, se aprecia un reporte de vulnerabilidades realizado a un servidor de la red. Puede apreciarse que se detallan bastante las vulnerabilidades encontradas, incluso se da una idea bastante oportuna del modo de solucionarla.

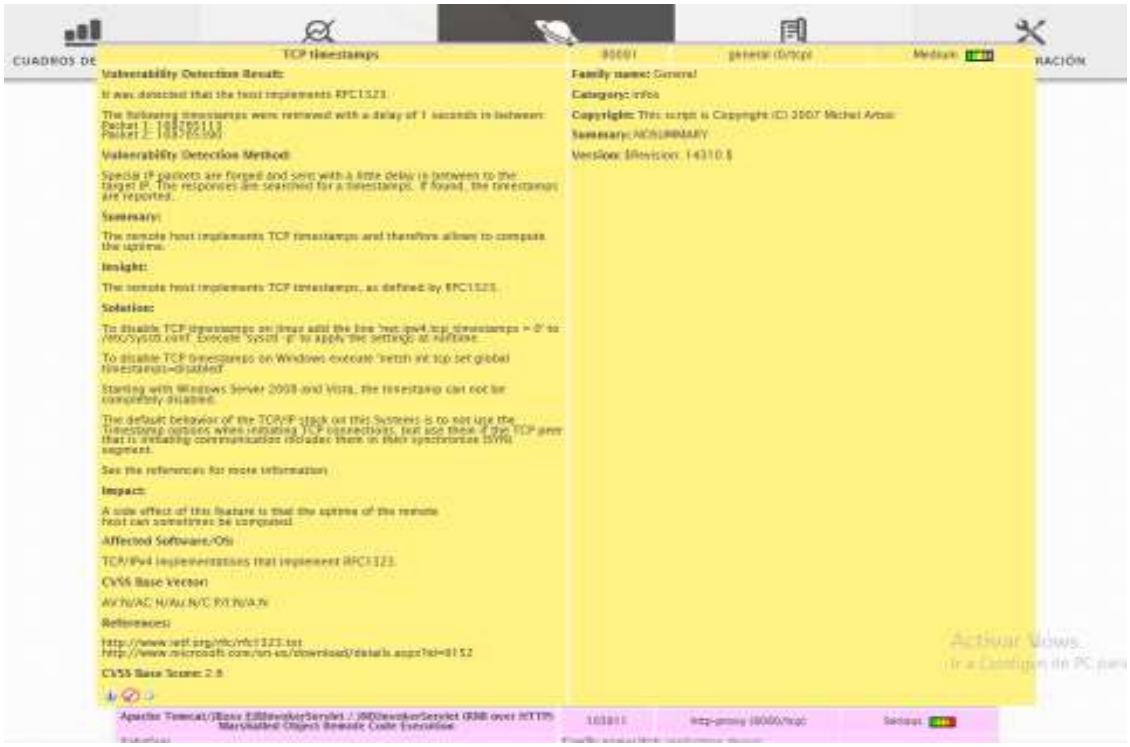

Figura 4. Ejemplo del reporte de una búsqueda de vulnerabilidades hecha a un servidor de la red de la Universidad de Granma.

Sistemas de resguardos y actualizaciones.

Las actualizaciones se han garantizado empleando repositorios para el sistema operativo Linux Fedora Core, que es la distribución más extendida en los sistemas de la red. También se utiliza el WSUS para los sistemas y estaciones de trabajo con Microsoft Windows.

Los resguardos se implementaron con Bacula, Baculaweb y Baculum. Bácula es una colección de herramientas de respaldo, capaces de cubrir las necesidades de respaldo de equipos bajo redes IP. Licencia de Software libre y código abierto y resulta independiente al Sistema Operativo. (Bacula.org, 2022)

El sistema fue configurado de manera que se realizaran resguardos automáticos y diarios de tipo incremental a todos los servidores existentes en los nodos o centros de datos de la UdG. También se realizan resguardos diferenciales durante los fines de semanas y resguardos completos, un fin de semana de cada mes.

También se emplean el Bacula Web, que es una interface liviana para monitorear los resguardos realizados, y el Baculum, otra interfaz web pero más compleja, que sirve tanto para monitorear como para configurar y manejar el sistema a más bajo nivel. (figura 5)

Es importante señalar que este sistema se diseñó de manera tal que en cada uno de los 3 centros de datos que existe, hay un servidor de esta clase, los cuales se realizan los resguardos de manera cruzada, es decir, un centro de datos realiza los resguardos de otro centro de datos. La figura 5 muestra la interface web de administración del sistema, mediante la cual se pueden monitorear la marcha diaria de los resguardos, crear nuevas configuraciones.

Finalmente se puede mencionar que actualmente los sistemas que alojan los servidores virtuales (hypervisors), también realizan copias de segurirdad semanales a los sistemas que alojan.

Sistema de firewalls.

El empleo de firewalls o cortafuegos comenzó justo en el año 2004, primero se empleó IPChain y posteriormente IPTables. En los útimos años se utiliza una combinación de IPTables, IPSet, las herramientas para el control de ancho de banda basadas en traffic shaping y tc.

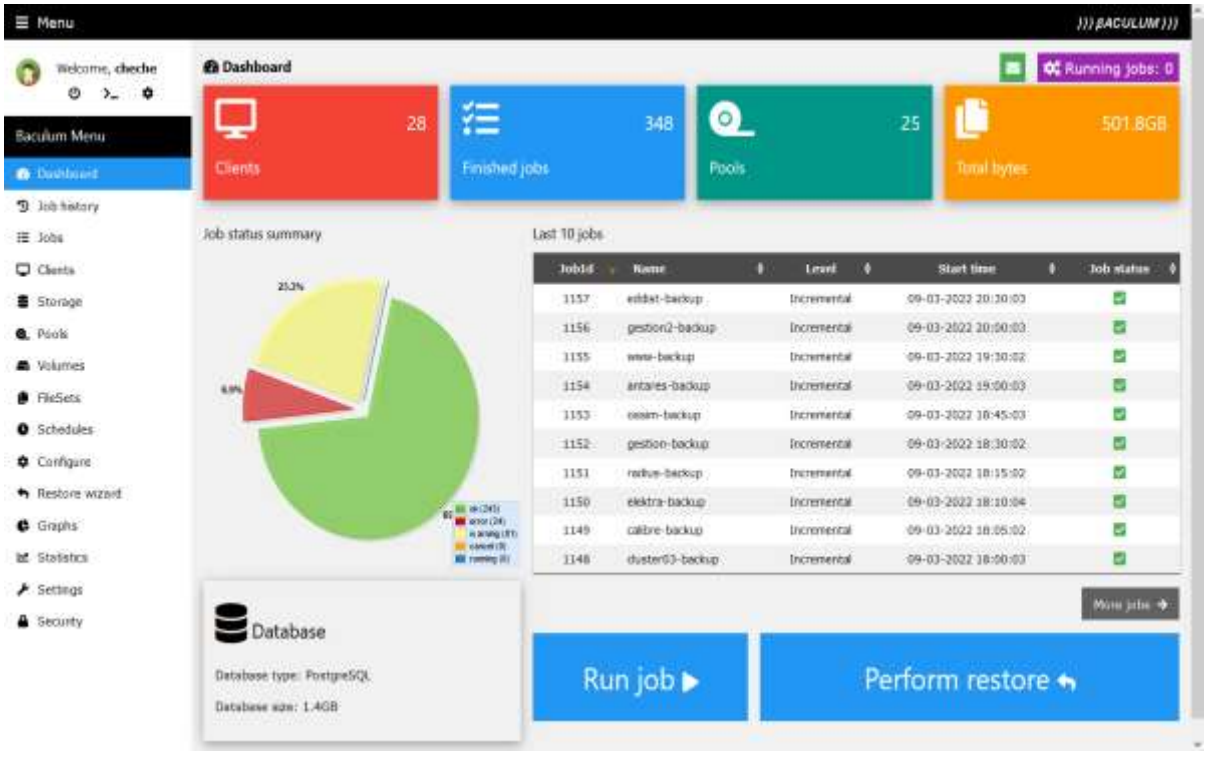

Figura 5. Interface de administración y gestión del sistema de resguardos (Baculum)

En este momento existe en el router de borde, basado en Cisco IOS, un firewall donde se analiza todo el tráfico entrante y saliente desde el exterior a la red local. Cada servidor,

tanto de la DMZ, como de la red interna de servidores, cuenta con servidores locales basados también en IPTables e IPSet. Existe un router – software, que interconecta todas las redes privadas de la universidad, tanto locales como remotas, éste es el firewall principal, basado en IPTables, IPSet, Traffic Shape, TC y IPTNetflow. (Figura 2)

Todas las aplicaciones antes mencionadas, tanto del Sistema de gestión, como de los sistemas de seguridad y resguardos, forman parte actitva del Sistema de seguridad Informática de la Red de la Universidad de Granma. Para ello, se muestra en la tabla 2, el modo en que cada una se puede emplear para minimizar algunos de los ataques más frecuentes que pudieran existir.

Tipos de ataque	Aplicaciones para detectarlo y contrarrestar sus efectos
Malware (Virus, Gusanos, Troyanos, Spyware, AdWare, Ramsomware, botnes)	• Educación de los usuarios (trabajo social), • Repositorios de actualizaciones, WSUS. • Sistemas antivirus actualizados. • Empleo del IDS con OSSIM. • Gestión de pérdidas de paquetes con SmokePing y nagios • Gestión de tráfico con NFSen, y Cacti. • Escaneo de vulnerabilidades utilizando OpenVas.
Email spoofing - Phishing	• Gestión del tamaño de las colas de correos (Nagios, Proxmox Mail Gateway, AWStats, SendmailAnalyzer)
Ataques por Denegación de servicios (DDoS)	• Gestión de pérdidas de paquetes empleando SmokePing • Gestión de tráfico: NFSen y Cacty
Escaneo de puertos, búsqueda de vulnerabilidades	• Filtrado de paquetes, sistemas de firewalls, IDU (OSSIM).
Intruciones no autorizadas	• Filtrado de paquetes, sistema de firewalls (IPTables, Cisco Firewall, Nagios para el chequeo de acceso a ciertas cuentas en los servidores).
Intentos de inyecciones SQL	• Uso de los IDS (OSSIM) para su detección, empleo de Firewalls para la protección de los sistemas de gestión de bases de datos, direccionamiento privado de éstos, etc.

Tabla 2. Eventos de seguridad más frecuentes en la Universidad de Granma: herramientas para su detección y acciones para neutralizarlos.

Actualmente la UdG cuenta con un sistema de seguridad desarrollado, científicamente fundamentado, dinámico y basado en normas y recomendaciones internacionales, el cual ha demostrado su eficacia, pues es de los pocos centros de educación superior cubanos que nunca ha tenido un incidente de seguridad severo, que haya provocado grandes pérdidas de información, grandes períodos sin servicios, etc.

Conclusiones.

- En este artículo, se ha realizado estudio descriptivo del modo en que surgió y evolucionó el sistema de seguridad informática de la red de la Universidad de Granma, describiéndose las condiciones que impulsaron su desarrollo.
- Hasta la fecha, los ataques más importantes, provienen tanto de la Red LAN de la Universidad, como de redes públicas.
- Desde que se han implementado los sistemas de seguridad, tienen lugar varias alarmas o alertas de seguridad y se reportan varios miles de eventos "sospechosos" diarios, entre los que se destacan intentos de inyecciones a servidores SQL de cualquier clase, ataques por correos phishing, búsquedas de servicios vulnerables y hosts remotos contaminadas por virus.
- En la medida que se aumente tanto la complejidad de una red como los servicios que ofrece, serán cada vez más costosos y complejos los sistemas de gestión y seguridad de la misma, pero en las condiciones actuales, donde la información es un valor de elevadísimo costo, la preservación confiable y segura de ésta, es una necesidad imperiosa, por lo que se justifican completamente todas las inversiones que se hagan para preservarla, por ello, es importante la creación de una consciencia que implique tanto a administradores de sistemas, como a directivos, en la necesidad de la implementación de un sistema de gestión que permita conocer a los especialistas, lo que sucede en la red que controlan.

Bibliografías

Bacula.org. (2022). Documentación de Bacula. from https://www.bacula.org/documentation/

Ding, J. (2009). *Advances in Network Management*: CRC Press.

Gómez, D., & González, A. (2013). *ARQUITECTURA PARA LA GESTIÓN DE SERVICIOS ADMINISTRADOS DE TECNOLOGÍA.* (MAESTRÍA EN

GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES SANTIAGO DE CALI). Retrieved from https://www.google.com.cu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjQ0Ma-tYzOAhWsyoMKHapCCbcQFggaMAA&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F41976485.pdf&usg=AFQjCNG10CEOGyucfCAewHnT26tAAtrTfA&bvm=bv.127984354,d.cWw

López, P. A. (2010). *Seguridad informática*: Editex.

Marrero, D., & Hernández, H. (2016). IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN PARA LA RED NACIONAL UNIVERSITARIA. *Trabajo de diploma para optar por el Título de Ingeniero en Telecomunicaciones y Electrónica), Instituto Superior Politécnico "José Antonio Echeverría*.

Nagios. (2022). Documentación oficial de Nagios. from https://library.nagios.com/

Pastor, F. (2015). Propuesta de política de gestión de capacidad para una compañía de tecnologías de la información de acuerdo con los requerimientos de ITIL. *3 Ciencias, 4*.

Pérez, L. (2013). ESTUDIO COMPARATIVO DE LOS SISTEMAS GESTIÓN Y MONITOREO BASADOS EN LOS REQUERIMIENTOS GENERALES DE LA RED DE UN CAMPUS UNIVERSITARIO. *Master en Redes de Comunicaciones), Pontificia Universidad Católica del Ecuador*.

Trujillo Alvira, J. O. (2022). Diseñar estrategias complementarias para mejorar la seguridad informática y de la información en la compañía QWERTY SA utilizando la norma ISO 27001.