Innovación y Software
ISSN: 2708-0927
ISSN: 2708-0935
facin.innosoft@ulasalle.edu.pe
Universidad La Salle
Perú

Rodríguez González, Ihosvany; Peña Casanova, Mónica; Bermudez Peña, Anié; Famadas García, Ariel O.; Blanco Domínguez, Alicia C.; Mauri Sedeño, Ludibel; Pérez Almario, Arley

Proyecto de gestión de redes en BioCen

Innovación y Software, vol. 2, núm. 1, 2021, Marzo-Agosto, pp. 64-82
Universidad La Salle
Perú

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículo original
Temática: Redes y seguridad informática
Recibido: 28/12/2020 | Aceptado: 05/03/2021 | Publicado: 30/03/2021

Proyecto de gestión de redes en BioCen

Network Management Project in BioCen

Ihosvany Rodríguez González [1][0000-0003-0212-9556]*, **Mónica Peña Casanova** [2][0000-0003-2500-4510], **Anié Bermudez Peña** [2][0000-0002-1387-7472], **Ariel O. Famadas García** [1][0000-0002-2199-4978], **Alicia C. Blanco Domínguez** [1][0000-0002-1713-1117], **Ludibel Mauri Sedeño** [1][0000-0001-5899-3859], **Arley Pérez Almario** [1][0000-0003-0588-0396]

[1] Centro Nacional de Biopreparados (BioCen). Mayabeque, Cuba. {ihosvany,fams,alicia,ludi,arley}@biocen.cu
[2] Universidad de las Ciencias Informáticas. La Habana, Cuba. {monica,abp}@uci.cu

* Autor para correspondencia: ihosvany@biocen.cu

Resumen
BioCen es una institución científica integrada por varias unidades productivas que se dedican a diferentes líneas en el universo biotecnológico y farmacéutico cubano. Para garantizar la seguridad y gestión de la información que se genera en la institución y minimizar el impacto de los riesgos asociados a fallas en la infraestructura, se cuenta con un conjunto de herramientas, procedimientos y estrategias, recogidas en un proyecto de gestión de redes que se actualiza todos los años. El proyecto recoge lo relacionado a la configuración, estructura, control y monitoreo, tanto de la red de datos, la de proceso, como de la wifi; además de la organización de los servicios, servidores, y los sistemas que los conforman. En este trabajo se presentan las herramientas de gestión utilizadas en BioCen para el control y monitoreo de los servicios que se prestan en la red, el tráfico interno y externo de la misma; así como la detección de incidentes. Se muestran ejemplos de monitoreo y control con las herramientas de gestión que se aplican en algunas áreas funcionales, así como el diseño de la red local de BioCen. Finalmente se abordan las pruebas realizadas al sistema de red, las auditorías internas, el análisis estadístico de los servicios y la respuesta a incidentes.

Palabras clave: gestión, biotecnología, infraestructuras tecnológicas, monitoreo y control, seguridad y red de datos.

Abstract
BioCen is a scientific institution made up of several production units that are dedicated to different lines in the Cuban biotechnology and pharmaceutical universe. To guarantee the security and management of the information generated in the institution, and to reduce the impact of IT risk, it has a set of tools, procedures and strategies, collected in a network management project that is updated every year. The project includes everything related to the configuration, structure, control and monitoring, both of the data network, the process network, and the Wi-Fi network; in addition to the organization of services, servers, and the systems that comprise them. This paper presents the management tools used in BioCen for the control and monitoring of the services provided on the network, its internal and external traffic; as well as the detection of incidents. Examples of monitoring and control are shown with the management tools that

are applied in some functional areas, as well as the design of the local BioCen network. Finally, the tests carried out on the network system, internal audits, statistical analysis of services and response to incidents are addressed

Keywords: *biotechnology, management, monitoring and control, security and data networks, technological infrastructure.*

Introducción

BioCen es una institución científica integrada por varias unidades productivas que se dedican a diferentes líneas en el universo biotecnológico y farmacéutico cubano: medios de cultivos y bases nutritivas, anti-anémicos, ingredientes farmacéuticos activos y productos parenterales. Además, dispone de otras áreas de servicios, entre ellas las de ingeniería, compras, aseguramiento de la calidad y control de la calidad. Para garantizar la seguridad y gestión de la información que en él se genera se cuenta con un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo, garantizar su integridad, disponibilidad y confidencialidad, recogidas en un proyecto de gestión de redes que se actualiza todos los años, cuyo objetivo central es logar la máxima disponibilidad de los servicios de la red, con los enfoques de negocio y técnico. Ello se realiza teniendo en cuenta las diferentes funciones al organizar la gestión como son: operación, administración, análisis y planificación. Elaborado a partir de las legislaciones establecidas en Cuba y cumpliendo las regulaciones internacionales establecidas para la Industria Biofarmacéutica.

El Proyecto recoge lo relacionado a la Red en BioCen, específicamente: la configuración, estructura, control y monitoreo, tanto de la red de datos, la de proceso, como de la wifi; además de la organización de los servicios, servidores y los sistemas que los conforman. Relacionando siempre cada servicio con las áreas funcionales de la gestión de redes y barriendo los componentes de un sistema integrado de gestión de redes y servicios.

El Departamento de Informática y Redes se encuentra subordinado a la dirección general, dando servicios y desarrollando productos para cumplir con los objetivos y metas de la empresa.

Materiales y métodos

BioCen cuenta con un sistema de gestión como se muestra en la Figura 1, el cual muestra una estructura por niveles y la estrecha relación que tienen para lograr una operación eficiente de la red y sus servicios.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

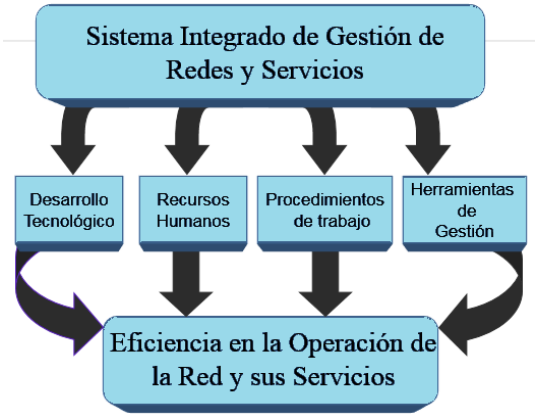

Figura 1. Sistema Integrado de Gestión de Redes y Servicios en BioCen.

En el desarrollo tecnológico se cuenta con la virtualización de varios servidores y *Cloud Computing* para el intercambio de información entre las empresas de BioCubaFarma, tenemos el servicio *VoD*, utilizando *Trueconf* para las videoconferencias, estamos comenzando un proyecto con España para elevar el estándar de BioCen a industria 4.0 y usar *IoT* en las plantas productivas. Además, solicitamos el incremento de ancho de banda de transmisión con el objetivo de mejorar las comunicaciones con cierta frecuencia y tecnología móvil 4G, entre otras.

Respecto a los recursos humanos se cuenta con un personal altamente calificado que siempre está superándose en las disciplinas y competencias que se necesitan para el buen desempeño de sus funciones, en especial los administradores de red y especialista de seguridad informática.

Se cuenta con un manual de procedimientos de las operaciones básicas para la gestión de la red y con un Sistema Certificado de Gestión de la Calidad a nivel de empresa, que rige el seguimiento y modificaciones de los mismos, para su actualización y mejoras.

Herramientas de seguridad en la red de BioCen

BioCen utiliza nueve herramientas de gestión (ver Figura 2) para el control y monitoreo de los servicios que se prestan en la red, el tráfico interno y externo de la misma; así como la detección de incidentes. La caracterización de cada sistema, su empleo y la frecuencia de monitoreo se reflejan en los informes de análisis diarios.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

Figura 2. Herramientas de seguridad utilizadas en la red de BioCen.

Los integrantes del grupo de redes son responsables de verificar los accesos de escritura y borrado a los subdirectorios de trabajos y carpetas, a través de programas que se ejecutan de forma automática y que informan de cualquier anomalía a los administradores de las aplicaciones. Se activan los medios de alarmas y avisos del sistema, que permiten a los operadores o administradores de los mismos, conocer cuándo están ocurriendo hechos relevantes según las reglas declaradas en cada caso.

Con el objetivo de implementar el cumplimiento de la Resolución 126/2019 del Ministerio de Comunicaciones "Medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas de datos" se establece el uso de las siguientes herramientas en la red de computadoras de BioCen:

1. Herramientas que muestran el estado actualizado de los servicios implementados en cada servidor.
    - PRTG Nerwork Monitor (versión 17). Su función es alertar sobre problemas en la red. Permite realizar chequeos intermitentes en los equipos y en los servicios que se especifiquen con el uso de complementos externos, los que devuelven información al sistema informático. Proporciona gran versatilidad para consultar cualquier parámetro de interés de un sistema y genera alertas que se reciben por medio de correos electrónicos y SMS, cuando estos parámetros exceden los márgenes definidos por el administrados de la red. Las alertas son recibidas y procesadas, según se presentes, por el administrador de red [1].
    - ManageEngine AD Manager Plus (versión 6) [2]. Permite a los administradores de redes administrar objetos de Active Directory (AD) fácilmente y general informes instantáneos. Se emplea por los administradores de la red en la gestión de usuarios y grupos del AD, según necesidad. Se aprovecha las facilidades de generación de informe para elaborar estadísticas de los servicios brindados o cualquier otra información solicitada por los administrativos o la especialista de seguridad informática.

- Kerio Control (versión 9) [3]. Es un firewall de gestión unificada de amenazas que cuenta con la prevención de intrusiones, filtrado de contenido, brinda informes de actividades y permite la gestión del ancho de banda. Es empleado por el administrador de la red en la gestión del servicio de internet diariamente. También es utilizado por la especialista de seguridad informática para la confección de informes estadísticos mensuales de la utilización de este servicio e investigación de incidentes.

2. Herramientas para supervisar la carga y disponibilidad de los servidores.
    - PRTG Network Monitor y ManageEngine AD Audit Plus (versión 6) [4]. Esta última es una herramienta que permite la monitorización de redes, vigilar los equipos y servicios que se especifiquen, así como alertar cuando su comportamiento no es el adecuado. Pueden realizar el monitoreo de los servicios de red (SMTP, POP3, HTTP, SNMP) y de los recursos de sistemas de hardware (carga del procesador, uso de los discos, memoria, estado de los puertos). El monitoreo es realizado semanalmente por el administrado de red.
3. Sistemas de detección y prevención de intrusos (IDS/IPS en inglés).
    - Open Source Security Information Management (OSSIM) (versión 5.8.6) [5]. Es capaz de generar análisis de tráfico en tiempo real y registro oficial de eventos (logs) de paquetes en redes IP. Protege los sistemas computacionales de ataques tanto internos como externos, de manera proactiva; con el uso de tecnologías de detección basada en firmas, en políticas, en anomalías o por medio de sensores. Los sistemas IDS/IPS son usados en conjunto. El monitoreo es realizado diariamente por el administrador de red.
4. Herramientas para monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías.
    - ManageEngine Netflow Analyzer (versión 12.4) [6]. Su función es monitorear el comportamiento del tráfico de la red, brinda gráficos de tráfico multi-enrutadores (MRTG en inglés), que permite monitorear la progresión del tráfico entrante o saliente de las interfaces del enrutador y el estado de la red, a partir del protocolo simple de Administración de red (SNMP). Contiene archivos de imágenes y proporciona una información visual en línea del tráfico de los dispositivos. El monitoreo es realizado diariamente por el administrador de red.
5. Herramientas para dar seguimiento a las trazas.
    - Kiwi Syslog Server (versión 9.6) [7], ManageEngine EventLog Analyzer (versión 12) [8], Kerio Control y Sawmill Enterprise (versión 8.7). Estas herramientas realizan análisis de logs y generan los

reportes asociados a los servicios media, e-mail, registros de seguridad, redes y de aplicaciones. Son herramientas que permiten a los administradores de sistemas informáticos ver de una manera sencilla y amigable qué sitios de Internet se visitan. Generan listados diarios, semanales, mensuales y personalizados con los sitios de Internet que visita cada usuario, cuánto consumió en megabytes, entre otras informaciones. Son empleadas por el administrador de red y la especialista en seguridad informática para monitorear diariamente, elaborar las estadísticas mensuales del uso de estos servicios y realizar la investigación correspondiente ante un incidente de seguridad detectado.

6. Herramientas para la detección de posibles vulnerabilidades en la red.
    - Open Source Security Information Management (OSSIM). Es empleada para explotar, administrar y auditor la seguridad de redes. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones que corren en ellos, su sistema operativo, así como qué cortafuegos corren en una red. Realiza un chequeo exhaustivo de potenciales problemas en el servidor, existencia de archivos y aplicación peligrosas. El monitoreo es realizado diariamente por el administrador de red y semanalmente por la especialista en seguridad informática.
7. Herramientas para el control centralizado del inventario de hardware y del software.
    - LanSweeper (versión 7.2) [9]. Es empleada para el control remoto por los administradores de redes del inventario de hardware y del software. Permite escanear una dirección IP o una subred con el objetivo de obtener información detallada de equipos no inventariados. Es empleada, según necesidad para el desempeño de sus funciones, por la especialista del grupo de informática que atiende el control del equipamiento, los técnicos de mantenimiento de hardware y software, así como por la especialista en seguridad informática para el monitoreo mensual e investigación de incidentes.
8. Gestión de actualizaciones de seguridad.
    - Windows Server Update Services (WSUS, 2019) [10]. La actualización las herramientas de seguridad es muy necesaria para eliminar los problemas de seguridad, lo cual permite mantener la eficiencia operativa y la estabilidad en la infraestructura de los sistemas. La supervisión es realizada semanalmente por el administrador de red.
9. Sistemas de correlación de eventos.
    - Open Source Security Information Management (OSSIM). Sistema que combine toda la información de las diferentes herramientas de seguridad para mostrar por medio de la correlación de eventos lo que sucede en la red en tiempo real. Esto le permite al supervisor tomar medidas con carácter proactivo

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

ante un evento o incidente de seguridad. El monitoreo es realizado diariamente por el administrador de red y semanalmente por la especialista en seguridad informática.

El diseño de la red de los centros de datos se basa en un modelo estructurado de tres capas, lo cual permite incrementar la escalabilidad, el rendimiento, la disponibilidad y el mantenimiento de forma transparente y continua (ver Figura 3). Cada una de estas capas requiere una funcionalidad diferente:

- Núcleo: conmutación en capa 3 del tráfico que entra y sale del centro de datos. Brinda conectividad a varios módulos de agregación. Se encarga del enrutamiento entre el centro de datos y la red externa.
- Agregación: brinda un punto de consolidación en el cual los *switches* de la capa de acceso se interconectan dando extensión a las *VLANs* entre servidores que estén en diferentes racks. Provee una frontera entre los enlaces capa 3 y los dominios de *broadcast* capa 2. Se encarga del procesamiento del STP, puertas de enlace redundantes. Brinda servicios como cortafuegos, detección de intrusos, balance de carga. Es la capa fundamental de un centro de datos.
- Acceso: conformado por los *switches* que les brindan conectividad a los servidores. Permiten mantener el tráfico de servidor a servidor dentro de una misma VLAN de forma local lo que reduce la necesidad de procesamiento en las capas superiores.

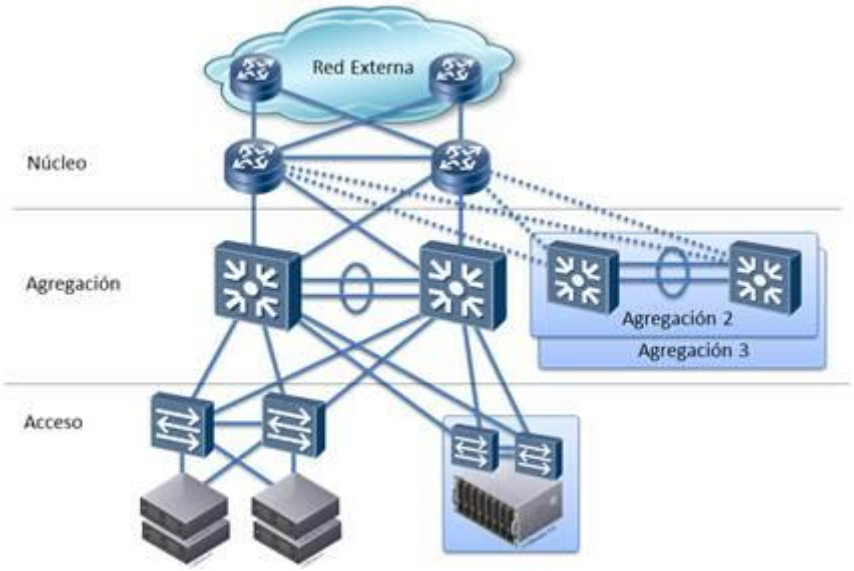

Figura 3. Diseño de la red de los centros de datos basado en tres capas.

Ejemplos de monitoreo y control

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

Ejemplos de monitoreo y control con tres herramientas de gestión que se aplican en algunas áreas funcionales, para su evaluación y análisis.

Gestión de contabilidad

La Figura 4 muestra una captura de pantalla con la herramienta PRTG sobre la recolección de datos estadísticos y utilización de los recursos.

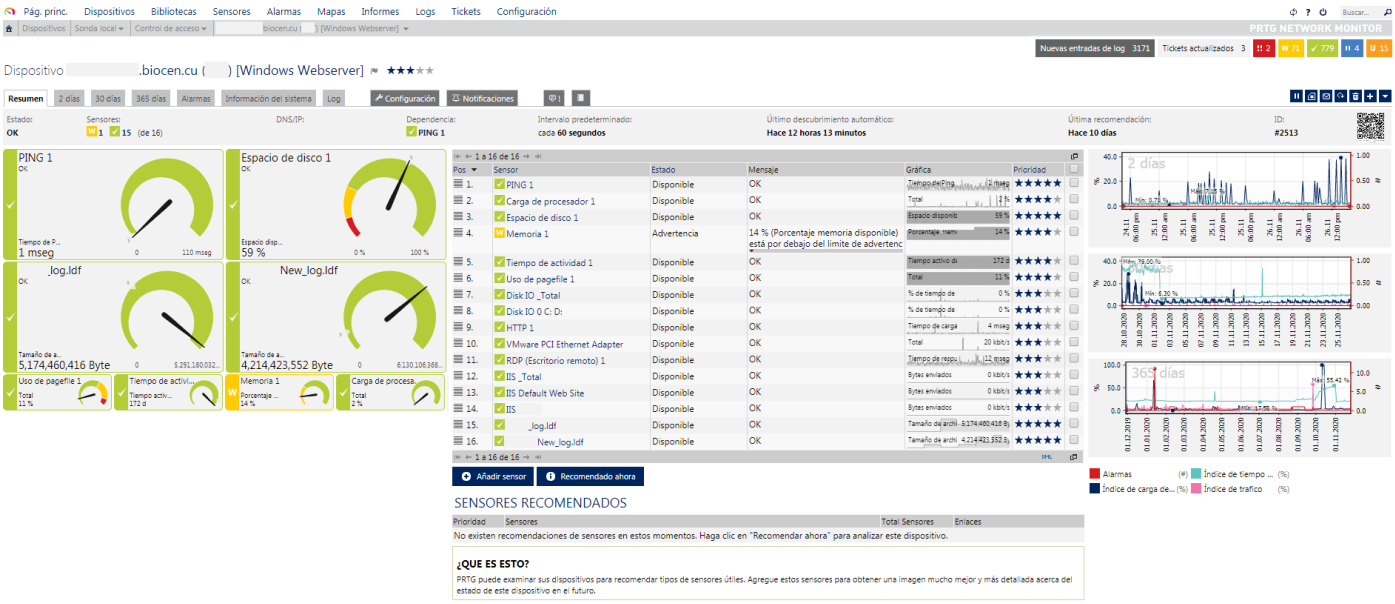

Figura 4. Ejemplo de recolección de datos estadísticos con la herramienta PRTG en BioCen.

La Figura 5 muestra una captura de pantalla con la herramienta PRTG sobre el monitoreo de la disponibilidad de los servicios y recursos de la red.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

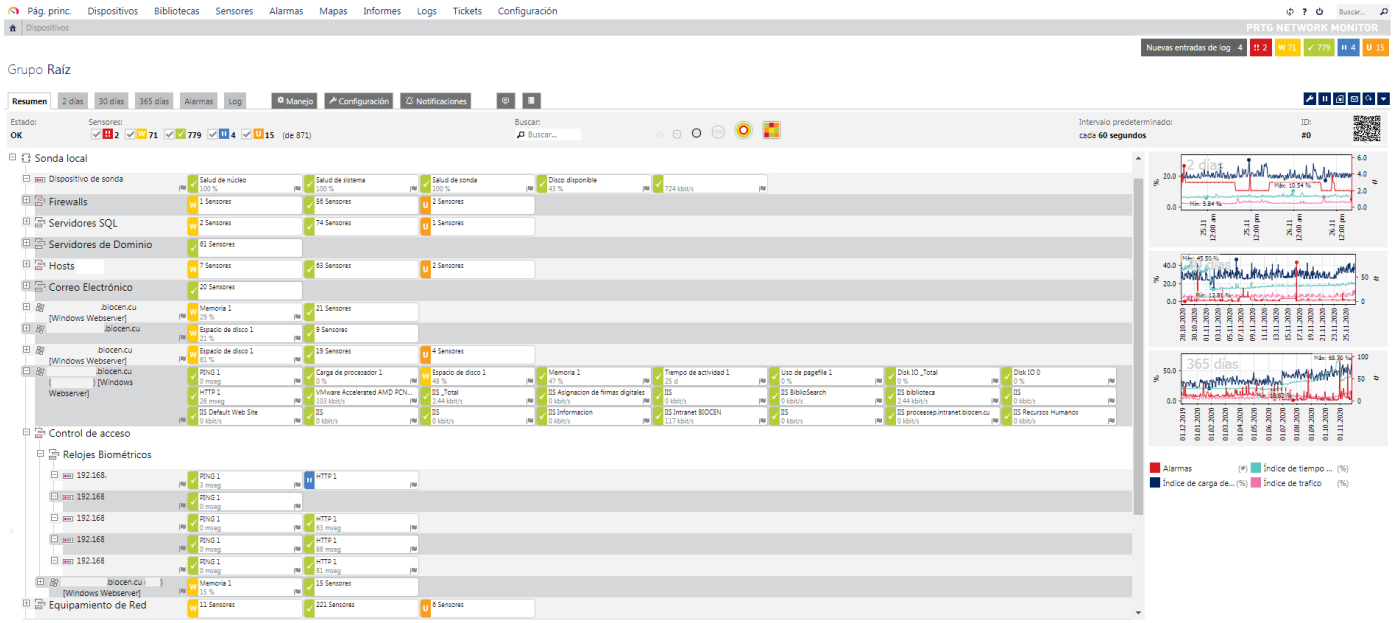

Figura 5. Ejemplo de monitoreo con la herramienta PRTG en BioCen.

La Figura 6 muestra una captura de pantalla con la herramienta Kerio Control, sobre el monitoreo de ancho de banda de Internet por direcciones en la empresa.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

Figura 6. Ejemplo de monitoreo con la herramienta Kerio Control en BioCen.

Gestión de rendimiento

La Figura 7 muestra una captura de pantalla con la herramienta PRTG sobre el ancho de banda del canal de la VPN de BioCubaFarma.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

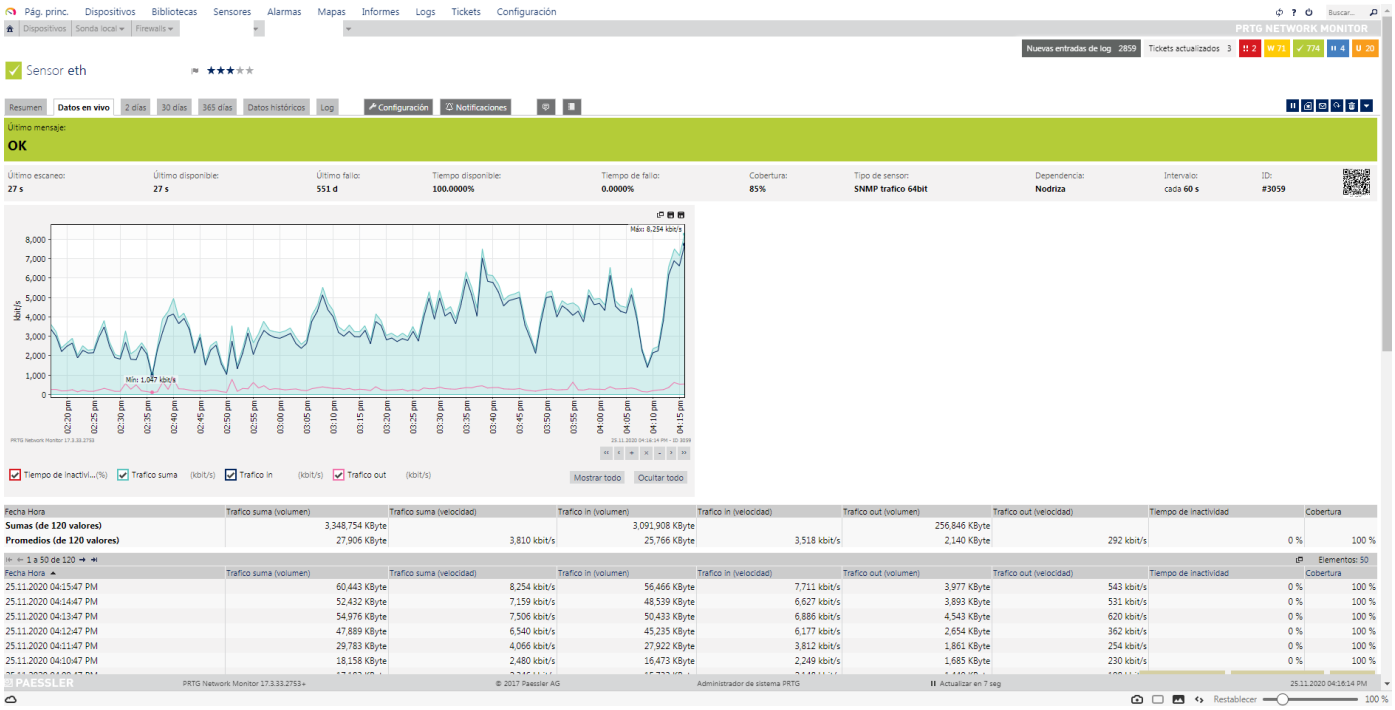

Figura 7. Ejemplo de gestión de rendimiento con la herramienta PRTG en BioCubaFarma.

Gestión de fallos

La Figura 8 muestra una captura de pantalla con la herramienta PRTG sobre las reglas para detectar fallos de umbral.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

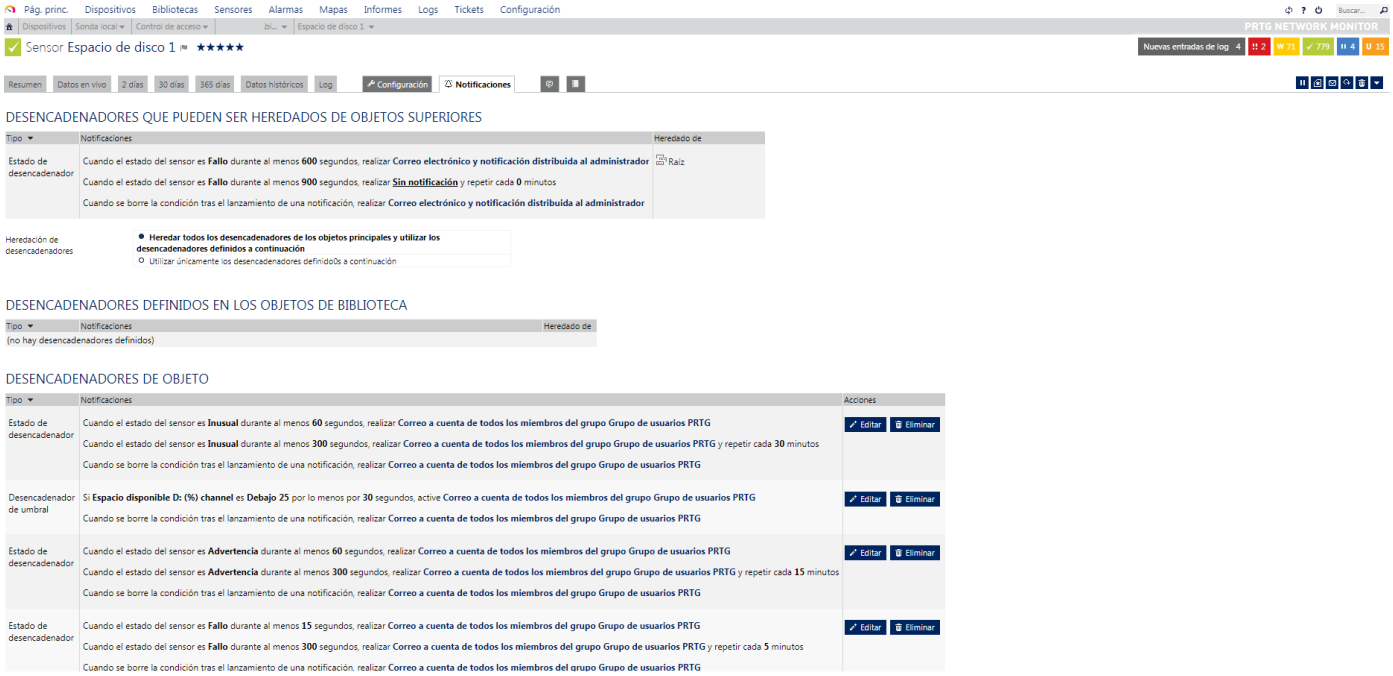

Figura 8. Ejemplo de gestión de fallos con la herramienta PRTG en BioCen.

Gestión de seguridad

La Figura 9 muestra una captura de pantalla con la herramienta OSSIM para el análisis de vulnerabilidades.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

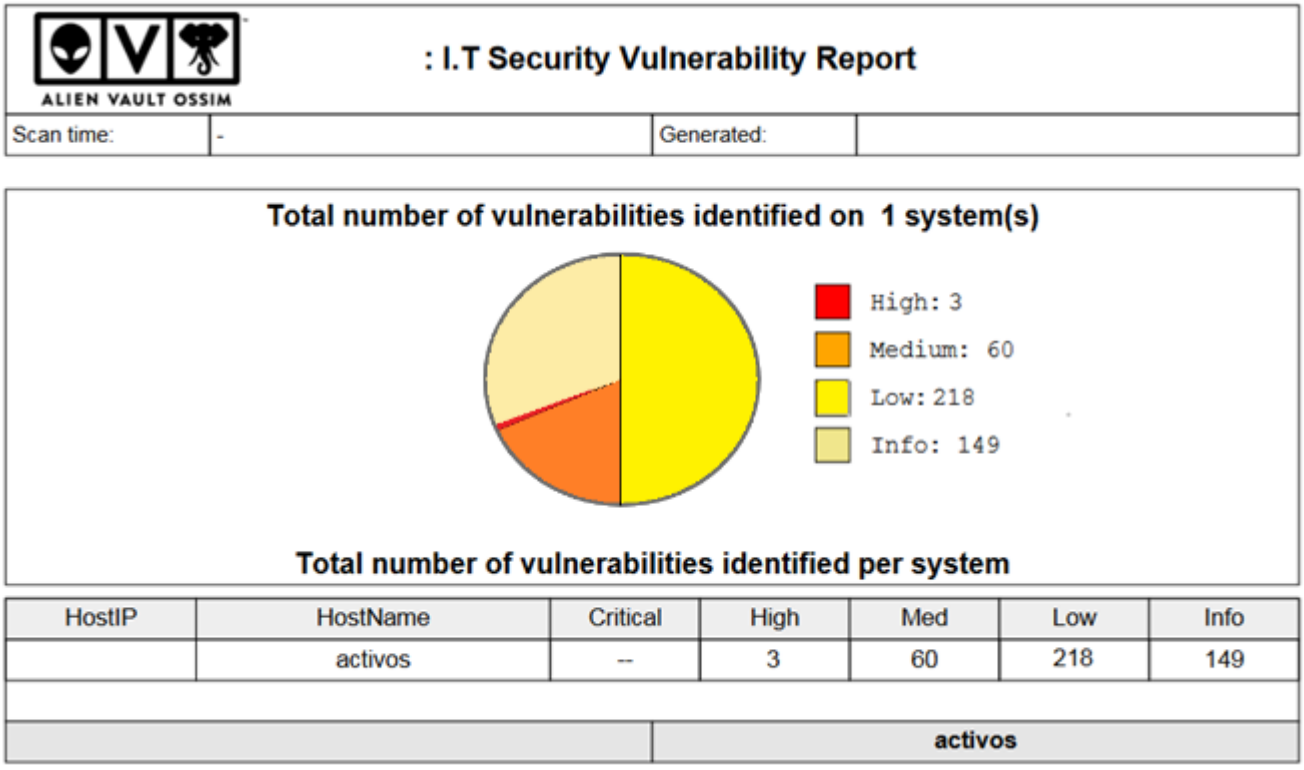

Figura 9. Ejemplo de gestión de seguridad con la herramienta OSSIM en BioCen.

Gestión de redes en BioCen

A continuación, se muestra la configuración de redes, la seguridad de servicios, auditoría, incidentes y algunos servicios disponibles para los usuarios de BioCen.

Configuración de la red, servicios y distribución del cableado

La Figura 10 muestra el diseño de la red local donde se aprecian algunas características. Posee un cableado central de fibra óptica para los exteriores y que enlaza a cada una de las edificaciones y cableado par trenzado para el interior de las instalaciones. Todos los servicios que se brindan están soportados en los servidores físicos y virtuales.

La entidad proveedora del servicio de conectividad para BioCen es la Empresa de Tecnología de Información (ETI), con la cual se ha establecido el contrato correspondiente, esta nos brinda los servicios de conectividad con la Red BioCubaFarma, así como, la navegación por Internet, servicios de bases de datos de información científica, acceso a la Nube, etc. La conexión contratada es protegida por un cortafuego administrado por nuestra entidad.

Revista Innovación y Software
Vol. 2, No. 1, Mes Marzo-Agosto, 2021
ISSN: 2708-0935
Pág. 64-82
https://revistas.ulasalle.edu.pe/innosoft

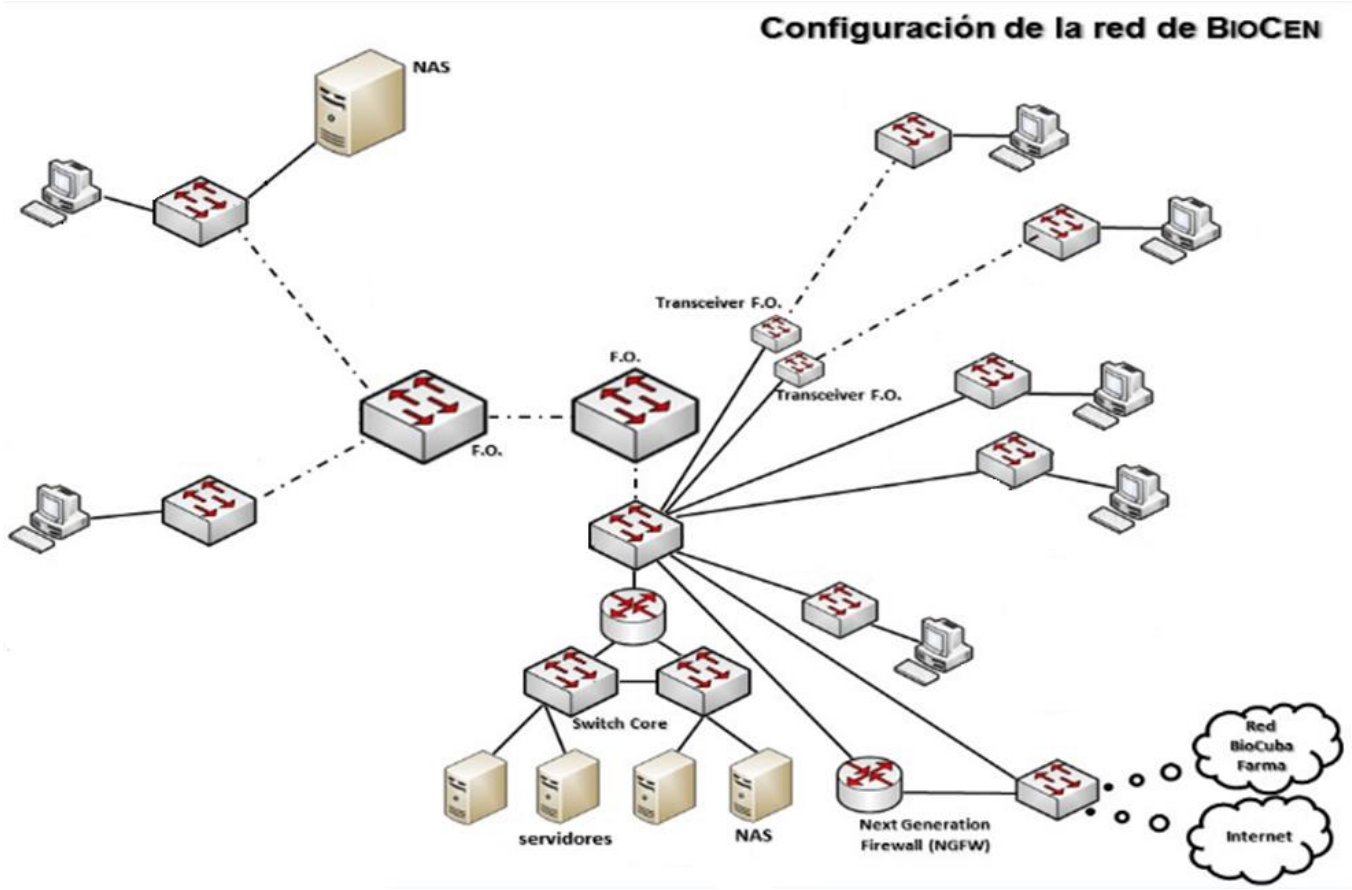

Figura 10. Diseño de la red local en BioCen.

Seguridad implementada en la sala de servidores

Todos los servidores están protegidos contra el ataque de virus informáticos con la instalación de antivirus propios para servidores, que se actualiza periódicamente de forma automática. Algunos servidores instalados con LINUX y otros con Windows Server.

Solo un grupo muy reducido de usuarios cuentan con privilegios especiales dentro de la red, la habilitación y control de este servicio es realizado a través de las Políticas de Acceso del Servidor Proxy utilizando el administrador del mismo. Se realizan salvas periódicas de la información contenida en los servidores, la cual se programa en dependencia del grado de sensibilidad para la Institución y la frecuencia de actualización de la misma, separándose en diaria, semanal o mensual. Los servidores cuentan con sistemas de protección eléctrica (UPS) que garantizan la continuidad del proceso informativo en casos de fallos de corriente eléctrica.

En situaciones de desastre existe un local climatizado en un edificio alejado del nodo central, donde tenemos equipamiento con las réplicas de todos los elementos crítico que tenemos en los servidores centrales.

Servicio de correo

BioCen cuenta con un dominio propio biocen.cu, registrado en el Centro Cubano de Información de Red (CUBANIC), CITMATEL, según contrato que se renueva anualmente; por lo que todas las direcciones de correo definidas en nuestro servidor salen con el sufijo @biocen.cu. Sólo tienen acceso al correo electrónico internacional los usuarios que han sido debidamente autorizados por la Dirección General del Centro. Esto es habilitado y controlado por el Administrador de Red a través de las facilidades que brindan las herramientas de administración del software que brinda este servicio.

Servicio de Internet

La conexión a redes externas se brinda a través de un router, que trabaja con una línea dedicada conectada a un equipo que realiza la transmisión de datos a través de fibra óptica dedicados para internet y conectividad nacional. La conexión a la red interna se realiza a través de un proxy con un corta fuego, que se mantienen actualizados. El control de la conexión se realiza por la coincidencia del nombre de usuario, dirección IP y número MAC correspondiente al hardware de cada estación de trabajo y en horarios establecidos para cada uno de ellos. Se registran todos los accesos a Internet y se monitorean periódicamente.

Los servicios son filtrados hacia el interior de la red aprovechando las facilidades de filtrado de paquetes con que cuentan los servidores Proxy. El servidor destinado a esta tarea está configurado de manera tal que:

- Se bloquean del exterior al interior todos los servicios que no se utilicen y los puertos correspondientes.
- No se permite la entrada de paquetes que contengan alguna de nuestras direcciones interiores como dirección de origen.
- Sólo se permite la salida hacia INTERNET de las estaciones de trabajo de los departamentos que hayan sido previamente autorizados a conectarse a INTERNET y verificando que coincida el número IP del ordenador con el usuario autorizado a utilizar este servicio desde él.

Servicio de acceso remoto

El servicio de acceso remoto se brinda vía MODEM que están dedicados al enlace desde el exterior de la Institución a la red como una terminal más. Este servicio está instalado en las estaciones de trabajo personales en los hogares de

directivos y especialistas principales de las direcciones, según necesidad Institucional y con la autorización del Director General.

Servicio de Acceso a la red mediante enlace Wifi

El servicio de acceso a la red mediante el enlace WIFI de equipos móviles, es autorizado solo por la máxima dirección de la entidad, la Directora General. En cada equipo se aplican las siguientes medidas de seguridad:

- Anclaje de IP a la MAC del móvil para conexión a la WIFI de BioCen.
- Acceso a Internet y Correo Electrónico empresarial por WorldClient mediante conexión segura.
- Configuración que Brinda la ETI para la conexión a la VPN de BioCubaFarma.
- Instalación de Antivirus.
- Instalación y configuración de Corta Fuego.

Auditorías al sistema de red

En BioCen se establecen diferentes tipos de inspecciones o auditorias, de forma tal que se abarcan todos los elementos que intervienen en la seguridad del sistema, las cuales están dirigidas a:

- La inspección se realiza en conjunto con la Especialista de la Oficina para el Control de la Información Clasificada (OCIC) de la Institución.
- Anualmente se realizan inspecciones internas a la seguridad implementada en los puestos de trabajo habilitados para el procesamiento de la IOC.
- Trimestralmente se realizan inspecciones a los controles y servicios implementados en la Red de BioCen.
- Se establece que anualmente los Activistas de Seguridad Informática de las áreas realizarán autocontroles para chequear el cumplimiento de las medidas definidas en el plan de seguridad informática.

Análisis estadísticos de los servicios

Mensualmente, utilizando las posibilidades de generación de estadísticas que poseen las herramientas para el monitoreo y control de los servicios de redes, se elaboran reportes de los servicios de Internet, correo electrónico y acceso remoto; las cuales incluyen los siguientes datos:

- Para Internet: Identificación de los usuarios, relación de los sitios más accedidos en el período en que se está monitoreando y cantidad de accesos realizados. Resumen del comportamiento de las categorías que pudieran indicar alguna incidencia o indisciplina, así como el análisis de las que se detecten.

- Para Correo Electrónico: Identificación de la cuenta, área a la cual pertenece, tipo de contenido (laboral u otros), cantidad de correos recibidos o enviados, así como los usuarios que más se comunican hacia el exterior. Se realiza un análisis de la racionalidad en el uso de este servicio y las cuentas implicadas en cualquier tipo de indisciplina detectada.
- Para el Servicio de Acceso Remoto: Se analizan los usuarios que utilizaron este servicio para detectar accesos no autorizados. Las estadísticas de los servicios son analizadas y procesadas, elaborándose un informe con los resultados del monitoreo.

Respuesta a incidentes

En caso de detectarse alguna anomalía en el uso de alguno de estos servicios que se brindan en BioCen, el mismo es interrumpido inmediatamente por el Administrador de la Red y se informa al Director del área a la que pertenece el usuario responsable del mismo, profundizando en el análisis de los elementos que causaron la misma. En caso de detectarse algún incidente de Seguridad Informática o violación de lo establecido, por cualquiera de las vías de auditoría o monitoreo, se procede según procedimiento establecido para esto.

Resultados y discusión

La importancia de una buena gestión de redes de datos

La gestión de redes de datos es un concepto amplio, que abarca su administración desde un enfoque completo. Dentro de ella se engloban políticas y procedimientos que intervienen en su planteamiento y configuración, así como el control y monitoreo de cara a evitar fallos y reforzar la seguridad, con el fin de asegurar la calidad de los servicios esperados.

La administración de redes, por lo tanto, es la suma de actividades orientadas a mantener una red eficiente, que tenga una alta disponibilidad. De ahí la importancia de llevar a cabo una buena gestión de redes de datos pues, en última instancia, un funcionamiento idóneo es un gran aliado para el buen funcionamiento de la empresa.

A mayor tamaño y complejidad de la red, más necesario será contar con un sistema de administración adaptado a sus necesidades, en el que se incluyan todos los aspectos relacionados con un adecuado funcionamiento. Solo así será posible prevenir y detectar problemas, incluyendo aspectos de seguridad, con la mayor anticipación posible, buscando minimizar errores.

Estándares y protocolos, un aspecto clave

Una buena gestión de redes de datos requiere, fundamentalmente, basarla en un modelo con tareas bien definidas sujetas a estándares y protocolos para facilitar tanto su implementación como su actualización.

En este sentido, cobran importancia los sistemas de gestión de redes de datos, al tiempo que se suele centralizar la gestión para vigilar el funcionamiento de la red o redes de la empresa.

Una diversidad que viene acompañada de protocolos y estándares. Su aplicación, por lo tanto, buscan ese control eficaz de la red para que ésta pueda responder en todo momento. En este contexto, existen distintos protocolos de gestión de red, algunos de ellos modelos estándar, como el SNMP que lo aplicamos en BioCen.

Conclusiones

Cada vez es más difícil llevar a cabo una adecuada gestión, capaz de dar acceso a los servicios que proporcionan las redes de datos de forma eficiente, pues estos también crecen en número y complejidad. Se trata de un reto que aumenta su dificultad conforme ganan en complejidad los sistemas de redes y, junto con ello, lógicamente se disparan las expectativas de funcionamiento. Afortunadamente, también la gestión de red ha ido evolucionando de forma paralela, a medida que han ido aumentando los diferentes servicios.

Como consecuencia de ello, este creciente desarrollo de servicios ha marcado la necesidad de gestionarlos convenientemente para que los usuarios puedan satisfacer sus necesidades sin interrupciones. A tal efecto, se precisan soluciones avanzadas, que monitoricen y automaticen procesos, así como buenas prácticas que ayuden a mejorar las capacidades necesarias en la entrega de servicios.

Actualmente nos encontramos ante un panorama diverso, si en sus inicios la gestión de red se basó sobre todo en la monitorización del tráfico de red, la detección de errores y el establecimiento de la calidad de servicio (QoS), en la actualidad disponemos de sistemas heterogéneos, lo que ha supuesto la proliferación de diferentes sistemas de gestión de red; donde se destacan los que emplean las técnicas de correlación de eventos que permiten en breve tiempo detectar fallas en el sistema e interrelacionar datos que cada día se vuelven más complejos. En BioCen se continúa mejorando nuestro sistema acorde como avance la tecnología, con el apoyo de la dirección de la empresa y la creación de nuevos proyectos sobre la gestión de redes.

Referencias

[1] T. Anttila, “WOIS Automation System Monitoring”, 2018.

[2] M. A. García Domínguez, “Intranet en centro de educación secundaria”, B.S. thesis, 2013.

[3] Z. Abidin, “LKP: Manajemen Proxy Server Berbasis Kerio Control pada Kantor Wilayah BPN Provinsi Jawa Timur”, PhD Thesis, Institut Bisnis dan Informatika Stikom Surabaya, 2018.

[4] S. Kamal, I. M. Helal, S. A. Mazen and S. Elhennawy, “Computer-Assisted Audit Tools for IS Auditing”, Internet of Things-Applications and Future, Springer, pp. 139-155, 2020.

[5] D. Karg, “Open source security information management (OSSIM)”, OSSIM, Standard Document, 2003.

[6] M. Engine, NetFlow Analyzer. Network Traffic Analysis with NetFlow. Available: https://www.manageengine, 2014.

[7] M. Ammar, M. Rizk, A. Abdel-Hamid and A. K. Aboul-Seoud, “A framework for security enhancement in SDN-based datacenters”, 8th IFIP international conference on new technologies, Mobility and security, pp. 1-4, 2016.

[8] F. Ö. Sönmez and B. Günel, “Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation”, International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, pp. 38-44, 2018.

[9] M. A. Hafsaoui and H. Mansour, “Développement d’une application de gestion du parc informatique”, PhD Thesis, Université Virtuelle de Tunis, 2019.

[10] D. Dimov, “Adaptive Patching Strategy”, Constanta Maritime University Annals, vol. 27, no. 223, 2019.