UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

MODELO DE SEGURIDAD DE GESTIÓN DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA EL DATA-CENTER DE LA FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS, EN LA UNIVERSIDAD TÉCNICA DEL NORTE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: CRISTIAN ALFONSO PERUGACHI ESPINOSA

DIRECTOR: MSc. CARLOS VÁSQUEZ

IBARRA, 2017

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de identidad	1004078943
Apellidos y Nombres	Cristian Alfonso Perugachi Espinosa
Dirección	Av. Atahualpa 26-62 y Cap. Espinosa de los Monteros
E-mail	cristianperugachi@hotmail.es
Teléfono fijo	062-650-991
Teléfono móvil	0998323225
DATOS DE LA OBRA	
Título	Modelo de seguridad de gestión de la información basado en la norma ISO 27001, para el Data-Center de la facultad de ingeniería en ciencias aplicadas, en la universidad técnica del norte.
Autor	Cristian Alfonso Perugachi Espinosa
Fecha	31/01/2018
Programa	Pregrado
Título	Ingeniera en Electrónica y Redes de Comunicación
Director	MSc. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Cristian Alfonso Perugachi Espinosa, con cédula de identidad Nro. 100407894-3, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar los derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Nombre: Cristian Perugachi

Cédula: 1004078943

Ibarra, Enero del 2018

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR

Yo, Cristian Alfonso Perugachi Espinosa, con cédula de identidad número 100407894-3 manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor del trabajo de grado con el tema: MODELO DE SEGURIDAD DE GESTION DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, EN LA UNIVERSIDAD TÉCNICA DEL NORTE. Que ha sido desarrollado con el propósito de obtener el título de Ingeniera en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Cristian Perugachi

100407894-3

Ibarra, del 2018

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MSc. CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN

CERTIFICA

Que, el presente Trabajo de Titulación: "MODELO DE SEGURIDAD DE GESTION DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA EL DATACENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, EN LA UNIVERSIDAD TÉCNICA DEL NORTE." Ha sido desarrollado por el Señor Cristian Alfonso Perugachi Espinosa bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

MSc. Carlos Vásquez

DIRECTOR

Dedicatoria

El presente trabajo está dedicado a mis padres, que gracias a su sacrificio y trabajo han sabido inculcarme valores morales y antes que nada ser una persona responsable lo cual me permitió culminar con éxito el primero de grandes logros.

A mis tíos y abuelos que desde un inicio han estado apoyándome y dando sus mejores consejos para salir adelante y no dejarme vencer en cualquier adversidad.

Agradecimientos

Dentro de lo concreto de este trabajo realizado he aprendido mucho de varias personas y tengo mucho que agradecer por la colaboración y la paciencia que ha tenido mi familia, amigos y docentes que han contribuido con su tiempo su paciencia y apoyo constante lo que permitió concluir pese a las dificultades concluir el trabajo iniciado y lograr las metas propuestas.

Quiero agradecer de sobre manera a mi madre que pese a los malos momentos estuvo a mi lado apoyándome cada día con todas las facilidades para dedicarme a elaborar el proyecto, también a mi padre que siempre estuvo tratando de ayudar a que finalizara lo que empecé.

Por último, quiero agradecer a una persona que siempre fue una luz en mi vida, pese a que no puede acompañarme hoy día, hoy llevo conmigo su recuerdo y las enseñanzas impartidas, se que ahora me acompaña en espíritu y espero que aun después de todo el tiempo que ha pasado siga sintiéndose orgullosa.

Índice

Índice de Figuras

Índice de Tablas

Resumen

El presente proyecto describe el proceso de elaboración de un modelo de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el Data-Center de la facultad de ingeniería y ciencias aplicadas, de esta manera estructurar políticas y controles basados en los lineamientos y objetivos de control presentados y orientados a la parte lógica de la arquitectura de red.

Se utilizo una caracterización de los equipos mediante la utilización de la metodología MAGERIT, la cual indica de forma cada fase de la recolección de información centrando su atención a la identificación de las características de los activos, la estructura organizacional, las amenazas y las salvaguardas que se encuentran implementadas en el centro de datos. Una vez realizado el proceso de caracterizar el escenario inicial se realiza un cálculo del riesgo potencial que indica si es necesario tomar acciones.

En la parte de diseño se procede a seleccionar las políticas y objetivos de control previstos en la norma ISO/IEC 27001 que mejor se adapten a la infraestructura, para responder de manera específica a cada objetivo se elaboraron manuales, procesos y se seleccionó Endian Firewall como el software a implementar.

Se puede constatar por medio de la aplicación de la metodología MAGERIT que los parámetros iniciales de riesgo para amenazas humanas accidentales y deliberadas se encontraban entre 8,6 y 9,3 respectivamente. Al implementar las políticas seleccionadas este riesgo se puede obtener que el riesgo disminuyera a rangos de 4,6 y 41 tanto en origen humano accidental y deliberado, lo que implica una mejora, pero no descarta que se elabore una planificación constante para mantener los niveles de riesgo bajos.

Capítulo I

Antecedentes

1.1. Planteamiento del Problema

La Facultad de Ingeniería en Ciencias Aplicadas acaba de implementar dentro de su infraestructura un Data-Center para alojar servidores y una red de servicios basados en el servidor de cloud computing privado.

El proyecto centrará su atención en lo que se refiere a la seguridad lógica de los servidores del Data-Center, entre los cuales se encuentran los servidores de cloud computing, un concepto nuevo dentro de las tecnologías de la información y que permite utilizar la virtualización de servidores para optimizar los recursos de la red de datos.

Se debe tener en cuenta que la topología de red en su diseño actual no contempla ningún tipo de seguridad además del firewall básico integrado en cada servidor, para los accesos LAN, WAN e internet hacia los servidores del Data-Center, permitiendo que se presenten los siguientes escenarios por acción de agentes internos o externos: ataques de denegación de servicio que incide en la disponibilidad de la información; ataques de suplantación de identidad afectando la confidencialidad de la información; infecciones de malware que incide en la integridad de la información.

Alojados dentro del Data-Center se encuentran servidores independientes y virtualizados que ofrecen aplicativos para interactuar con los usuarios finales de la red de datos, pero no se han realizado pruebas de monitorización que determinen la capacidad de flujo de datos soportado, ni de los puertos utilizados por cada uno de los servidores.

Las políticas de seguridad en el Data-Center no están establecidas, lo cual genera que los cambios realizados en la topología de la red para agregar, eliminar y modificar no cumplan con

un procedimiento estandarizado en base a normativas internacionales de seguridad, las que establecen además plan de acción en caso de existir vulnerabilidades en la seguridad lógica.

1.2. Objetivos

1.2.1. Objetivo General

Realizar el diseño de un modelo de gestión de seguridad de la información basado en la norma ISO 27001 para el Data-Center de la Facultad de Ingeniería en Ciencias Aplicadas.

1.2.2. Objetivos Específicos

Investigar las normas utilizadas para la implementación de sistemas de gestión de seguridad de la información en relación a la norma ISO 27001 y su evolución en relación a las TICs.

Evaluar las condiciones de los servidores del Data-Center para encontrar amenazas en la seguridad mediante la aplicación de los parámetros de control especificados dentro de la norma ISO 27001.

Establecer la metodología del sistema de gestión que permita el planteamiento de políticas en base a formatos de control, administración y auditoria en los servidores del Data-Center de manera lógica.

Implementar un sistema de gestión de seguridad de la información para los servidores integrados en el Data-Center evaluando los equipos disponibles que posee en referencia a la norma ISO 27001, especificando las pruebas de funcionamiento del software seleccionado.

1.3. Alcance

El presente proyecto plantea el diseño de un modelo de gestión de seguridad de la información para los servidores integrados en el Data-Center, se aplica la norma ISO 27001

pero centrando sus objetivos de control en la parte lógica de la red, para esto se realizara una monitorización del flujo de datos identificando el tipo de información, el tipo de usuario y las posibles vulnerabilidades en los servidores alojados que podrán afectar la confidencialidad, integridad y disponibilidad de la información.

Se realizará el desarrollo del marco teórico acerca de la seguridad en redes, antecedentes, evolución y métodos utilizados para cumplir con los objetivos centrales de la seguridad de la información que se enfocan en mejorar la disponibilidad, confidencialidad e integridad de los datos, además de investigar las normas utilizadas comparándolas en base a la norma utilizada para el desarrollo del presente proyecto.

El proceso a realizarse para comprobar las características de los servidores es un levantamiento de información para caracterizar las condiciones iniciales del Data-Center. Además, se realizará una verificación de los equipos disponibles de manera física, sus interfaces de comunicación y su capacidad de almacenamiento mediante las hojas técnicas de cada uno de los servidores si aún se encuentran disponibles, caso contrario se procederá a evaluar directamente los equipos.

Se diseñará un manual completo de políticas en base a la norma ISO 27001 teniendo en cuenta que todo cambio en la seguridad lógica del Data-Center seguirá un proceso de desarrollo, planificación, aprobación e implementación. Estas políticas generan formatos de procedimiento para las personas encargadas de cada uno de los servidores.

Dentro del diseño del SGSI en base a las condiciones actuales de la red se implementará un software que permita gestionar la red indicando por medio de un interfaz la interacción lógica de cada uno de los servidores, el flujo de datos que recibe y transmite, los puertos que está utilizando y las peticiones a la información realizados.

Se implementa en base a la situación actual las reglas para mantener un sistema de seguridad perimetral mediante un firewall ubicado de manera física externamente a los switch

de distribución del Data-Center que proteja puertos vulnerables utilizados por las aplicaciones alojadas en cada uno de sus servidores, así como el sistema de control de acceso lógico de los usuarios, se tramitara el auspicio de la institución de educación superior para el costo del firewall, en caso de no conseguirlo se lo asumirá mediante una inversión personal.

Se realizarán pruebas de funcionamiento para comprobar la utilidad del sistema implementado verificando las políticas implementadas por medio de software en la infraestructura y se presentarán los resultados obtenidos.

Según el manual de políticas y procedimientos se establece parámetros y buenas prácticas a realizar en caso de: existir amenazas en la seguridad de la información dentro de los servidores integrados en el Data-Center; realizar procesos de control, supervisión, configuración y modificación de servidores.

El análisis costo/beneficio será desarrollado en base al software o hardware utilizado en el desarrollo del proyecto y se resaltaran los beneficios que ofrece la implementación de la herramienta a la infraestructura del Data-Center.

1.4. Justificación

Los aplicativos implementados en los servidores del Data-Center de la facultad de ingeniería en ciencias aplicadas, presentan alternativas a los estudiantes docentes y administrativos para interactuar con las TICs, presentando entornos didácticos y modernos para la realización de actividades de aprendizaje, investigación, desarrollo, evaluación y socialización de información relacionada con la educación impartida en las aulas de clase. La seguridad dentro de la información compartida por este tipo de plataformas es un pilar importante para su correcto funcionamiento debido a que se debe garantizar por medio de cumplimiento de normativas los datos recibidos y transmitidos, mientras mayor seguridad mejor será el rendimiento de la red lo que se reflejará en la satisfacción del usuario

Según la norma ISO 27001 existen parámetros para garantizar la seguridad de información que está detallado en los objetivos de control de la normativa para que un SGSI pueda garantizar la confidencialidad, integridad y la disponibilidad de los datos.

Al afrontar la seguridad del Data-Center esta norma permite que cada incidente que atente a la integridad de los datos sea afrontado por medio de un proceso estructurado en base al manual de políticas y procedimientos. Incidiendo directamente en mejorar las prestaciones de los servicios brindados al usuario final, además de reducir costos de mantenimiento y perdidas de información.

El enfoque actual de las tecnologías plantea integrar todo tipo de servicios dentro de plataformas digitales, servidores virtualizados que permiten abaratar costos de implementación y costos de mantenimiento, así como brindar más servicios con una infraestructura de menor tamaño y menor cantidad de equipos. Al tratarse de servidores que interactúan con el usuario final, es importante definir normativas que regulen la seguridad de la información transmitida dentro de la intranet como internet, eventualmente al escalar la red en base a normativas se lograra una óptima utilización del recurso ofrecido por parte del administrador del Data-Center.

Capitulo II

Fundamentos Teóricos

2.1. Normativas de seguridad de la Información

En lo que a seguridad de la información se refiere existen normativas que permiten solucionar problemas de fondo en nuestras redes de datos y asegurar la confidencialidad, integridad y la disponibilidad. Teniendo en cuenta los avances tecnológicos los procesos de seguridad deben constantemente evolucionar para prevenir incidentes, dentro de las normativas más utilizadas se encuentra COBIT, ISO 27001, e ITIL.

2.1.1. COBIT

2.1.1.1.Antecedentes

Se constituyó por primera vez en el año 1995 como un estándar global que pudiese tener un amplio alcance en los negocios y sus controles de los sistemas de información, su primera edición fue publicada en 1996 y alcanzo 98 países de todo el mundo.

Su segunda edición se publicó en 1998 con varias mejoras fundamentales, agregados y revistas detalladas acerca de los objetivos de control de alto nivel, vino junto con un CD-ROM con la totalidad de su contenido.

2.1.1.2.Descripción

Es un conjunto de herramientas de gobierno de TI que permite a los administradores de una empresa encontrar una armonía entre los requerimientos de control, aspectos, técnicas y riesgos de negocios.

Brinda un modelo para la auditoria de gestión y control de los sistemas de información, además de todos los sectores relacionados con los administradores de las tecnologías de la información.

Según ISACF en su publicación oficial de Marco referencial COBIT (COBIT FrameWork) su misión es: "Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y generalmente aceptados para el uso cotidiano de gerentes de empresas y auditores". El beneficio directo para los auditores y administradores de red se basa en el entendimiento de las características y procesos que de su propio entorno relacionado a las tecnologías de la información, además de una constante monitorización y desarrollo.

2.1.2. ISO 27001

2.1.2.1.Antecedentes

- Se publicó como estándar internacional por la Organitation for Standarization y la comisión internacional Electrotechnical Commission en octubre del año 2005.
- Este estándar o norma es el resultado de la evolución de varios estándares de seguridad de la información, los cuales son:
- Normas “BS” (1901) publicadas por el British Standards Institution con carácter de internacional.
- BS 7799-1 (1995) Mejores prácticas para ayudar a las empresas a administrar la seguridad de la información, no se agregó una certificación ni una manera de conseguirla.
- BS 7799-2 (1999) Agrega los parámetros para conseguir una certificación.
- ISO/IEC 17799 (2000) La Organización Internacional para la Estandarización (ISO) utiliza los parámetros de la BS 7799-1.

- BS 7799-2 (2002) Se agrega la acreditación internacional.
- ISO/IEC 27001 (2005) Aparece la normativa como estándar internacional certificable.
- ISO/IEC 27001 (2007) Nueva versión.
- ISO/IEC 27001 (2009) Documento adicional con modificaciones leves a la norma.
- ISO/IEC 27001 (2013) Evolución de la norma en estructura, evaluación y tratamiento de riesgos.

2.1.2.2.Descripción

La norma se refiere a garantizar la seguridad de la información en todos los aspectos que abarca la misma, es decir la seguridad tanto física como lógica de los datos, para esto la normativa plantea varios objetivos de control los cuales deben ser establecidos e implementados siguiendo un plan de desarrollo constante y evolutivo, además de ser necesario contar con políticas de seguridad de la información.

El objetivo principal de esta normativa es garantizar las propiedades de la información que son confidencialidad, integridad, disponibilidad de los datos para de esta manera asegurar el activo más importante de una empresa o institución que son los servicios e información de la base de datos.

2.1.3. ITIL

2.1.3.1.Antecedentes

Se desarrolló en 1980 por la Agencia Central de Telecomunicaciones y Computación, actualmente Ministerio de Comercio en Reino Unido, dentro de este proyecto se involucraron varias firmas de consultoría para documentar las mejores prácticas para la infraestructura de TI, mientas el proyecto iba evolucionando tomo el nombre de ITIL.

Desde su origen fue puesta a disposición en modo de varios libros para de esta manera permitir que cualquier organización del mundo pudiera adoptarla, su primera versión consistía de 10 libros principales y varios complementarios, en 2001 se juntó 19 libros principales en 2 y los demás temas se mantuvieron separados para completar un total de 7 libros en su segunda versión.

En 2007 se revelo su tercera versión que consta solo de 5 libros que están estructurados en base al ciclo de vida de un servicio.

2.1.3.2.Descripción

ITIL o Biblioteca de Infraestructura de Tecnologías de Información es un marco de mejores prácticas para facilitar la entrega de servicios de tecnologías de la información de alta calidad, son una guía para toda la infraestructura, desarrollo y operaciones de TI.

Está basado en proceso-modelo de control y gestión de las operaciones, se creó para solucionar problemas de implementación de TI en organizaciones que a menudo salían más costosas, y tiene un glosario de términos completo.

El objetivo es lograr adaptación con los procesos y temas organizacionales de los servicios de TI, con un glosario estandarizado para describir los procesos de administración de servicios y llegar a una certificación.

2.1.4. Comparación COBIT, ITIL e ISO 27001

Tomando en cuenta el ciclo PDCA (Plan, Do, Check, Act) se encuentra las características y objetivos definidos por cada normativa para cada uno de los parámetros establecidos, esta caracterización se presenta en la Tabla 1.

Tabla 1.
Características y objetivos según PDCA para ISO, ITIL y COBIT

CICLO PDCA	**ISO 27001**	**ITIL**	**COBIT**
Planificar	Contexto de la información. Liderazgo Planificación Soporte	Estrategia del servicio. Diseño del servicio	Marcos específicos de controles /estándares
Hacer	Funcionamiento	Transición del servicio. Operación del servicio	Administrar TI Administrar la estrategia. Administración de presupuestos y costos. Administrar la seguridad
Verificar	Evaluación del desempeño	Servicio de mejora continua	Evaluación, monitoreo y cumplimiento Evaluación, monitoreo, sistema de control interno Evaluación, monitoreo, requisitos externos.
Actuar	Clausula 10.- Mejora continua	Servicio de mejora continua	Ambiente externo, estándares y seguridad

Fuente: Realizado por el autor

En un comparativo general de las normativas se define las características en la Tabla 2.

Tabla 2.
Comparativa entre la norma ISO, ITIL y COBIT

	ISO 27001	ITIL	COBIT 5
Versión Implementación	ISO 27001-2013 La implementación y certificación son opcionales	ITIL edición 2011 La implementación no está sujeta a la certificación	COBIT 5 2012 Sistema de auditoria de Información
Certificación	Opcional	Opcional	Obligatoria
Aplicación	Se aplicar en cualquier tipo de organización	Se aplica en casi todos los entornos TI	Cualquier tipo de organización TI
Función	Marco de seguridad de información	Mapeo de TI, nivel de servicio de Información	Mapeo de procesos TI
Consultoría	Consultoría TI, seguridad, consulta de red	Consultoría TI	Contabilidad, consultoría TI
Área	10 dominios	9 procesos	4 procesos y 34 dominios

Fuente: Realizado por el autor

En base al análisis general de las normativas se puede sacar las siguientes conclusiones:

- Cobit es una normativa que abarca todas las áreas relacionadas directa o indirectamente con las TI dentro de una organización, no se puede aplicar a una parte focalizada de la empresa o a un centro de datos especifico al momento de implementarla se debe aplicar todos sus controles o principios fundamentales y es requisito obligatorio una certificación.
- ITIL e ISO 27001 se pueden complementar entre ellas en algunos aspectos, ITIL se enfoca en los procesos para implementación y auditoria, en su lugar ISO 27001 centra la mayoría de sus objetivos de control en mejorar la gestión en seguridad de la información, se enfoca en ciertos parámetros que inciden en mejorar la integridad, disponibilidad y confiabilidad de los datos.
- En el proyecto se aplica la normativa ISO 27001 por la flexibilidad al momento de seleccionar los objetivos de control de manera focalizada que incluyen la implementación de políticas de seguridad dentro del Data-Center y mejoramiento de los parámetros de seguridad de la información.
- Hay que hacer énfasis que las tres normas pueden coexistir entre ellas pero para aplicarlas hay que pensar en la estructura de la red de datos universitaria, a cada centro de datos se le puede aplicar la normativa ISO 27001 o ITIL de manera independiente, pero al momento de generar políticas generales que regulen todos los centros de datos y al personal humano encargado del soporte, mantenimiento y control de la red e infraestructura se aplicara COBIT como un gestor de todas las TI dentro de la organización.
- Las tres normas pueden coexistir entre ellas, pero para aplicarlas hay que pensar en la estructura de la organización comenzando por implementar ITIL e ISO-27001 para los niveles inferiores.

2.2.Norma ISO 27001

2.2.1. Descripción

Este estándar es un conjunto de requerimientos y procesos necesarios para establecer, implementar y mejorar continuamente un sistema de gestión de seguridad de la información.

Se puede destacar que la normativa no limita el software que se debe implementar, pero si identifica los requisitos necesarios para su selección u optimización, se puede aplicar del mismo modo para el hardware, y el desarrollo de políticas las cuales son indicadas de manera general en la norma ISO 27002 permitiendo adaptarse al sistema integrado en cada una de las organizaciones sin importar su tamaño o función.

Como principio fundamental se encuentra mejorar la disponibilidad integridad y confidencialidad de la información mediante un proceso de administración de riesgos y planes de acción y evaluación.

El orden con que se presentan los dominios u objetivos a cumplirse no definen su importancia, cada ítem está relacionado a una parte de la organización, el administrador de la red tiene la libertad de seleccionar los dominios aplicables según su organización.

Dentro de los beneficios que ofrece la normativa son los siguientes:

- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos
- Confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información
- Flexibilidad para adaptar los controles a todas las áreas de su empresa o solo a algunas seleccionadas
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos

- Demostrar conformidad y conseguir el estatus de proveedor preferente
- Alcanzar las expectativas demostrando conformidad

2.2.2. Objetivos de control y controles

"En la normativa para la implementación de un sistema de gestión de seguridad de la información se encuentran los siguientes objetivos y controles orientados a la parte lógica de la seguridad de la información (Ver objetivos de control y controles de la norma ISO 27001 orientados a la seguridad lógica de la red en el Anexo A)"

Para la implementación de la normativa los objetivos de control se encuentran detallados en la norma ISO 27002, la cual consiste de 15 dominios encargados de separar y organizar todo lo relacionado a la seguridad de una infraestructura de red tanto en su parte de recursos humanos y los lineamientos lógicos y físicos de la red.

2.2.3. Modelo PDCA

Para mejorar la seguridad de la información la organización debe plantearse un modelo de gestión de seguridad de la información, lo que se busca con este modelo es proteger la información identificando todos los activos que deben ser resguardados y a que niveles.

Conforme a esto se debe aplicar el plan PDCA (Plan, Do, Check, Act), planificar, hacer, verificar y actuar para realizar un ciclo continuo mediante el cual se puede seguir mejorando, esto se comprende porque los riesgos nunca desaparecen en una red de datos y las relativas seguridades deben seguir mejorando en referencia a las amenazas, en la Figura 1 se observa el ciclo.

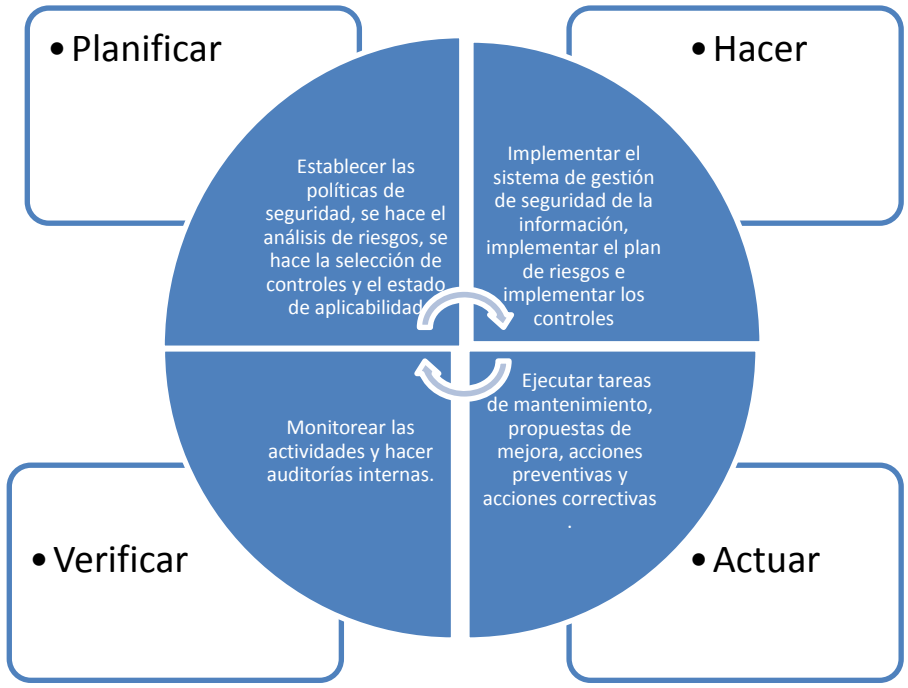


Figura 1. Modelo PDCA
Fuente: Elaborada por el autor

2.2.4. Políticas de Seguridad

Las políticas son instrucciones documentadas que indican cómo se llevara a cabo determinados procesos dentro de una organización, dentro de la misma también tiene su formato de elaboración de actividades, además de un organigrama de tareas a realizarse.

Se puede considerar las políticas como un documento obligatorio para las personas que trabajen dentro de la organización, además de incidir indirectamente con las personas externas que utilizan los servicios de la organización, además regulan los procesos que permitan proteger la información de los centros de datos de la organización.

2.1.Seguridad de la información

Es el conjunto de métodos organizativos y legales que permiten a una organización garantizar la confidencialidad, integridad y disponibilidad de sus sistemas de información.

En el pasado las organizaciones almacenaban la información por medio de documentos y se generaban archivos físicos extensos que ocupaban cuartos enteros, hoy en día con la digitalización de la información se puede reducir el espacio físico de almacenamiento, pero

aumentando los riesgos de seguridad por lo cual las técnicas han evolucionado constantemente para impedir perdida, robo o alteración de los datos.

En base a esto la norma ISO 27001, en su versión 2013 entrega el siguiente concepto.

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio."

Como se puede notar para asegurar la información existen parámetros que no solo se enfocan en una parte de la organización, además engloba todos los ámbitos y actores relacionados con los centros de datos.

2.1.1. Metodología de análisis de riesgos

La gestión de riesgos es una piedra angular en las guías de buen gobierno, público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riegos que implican.

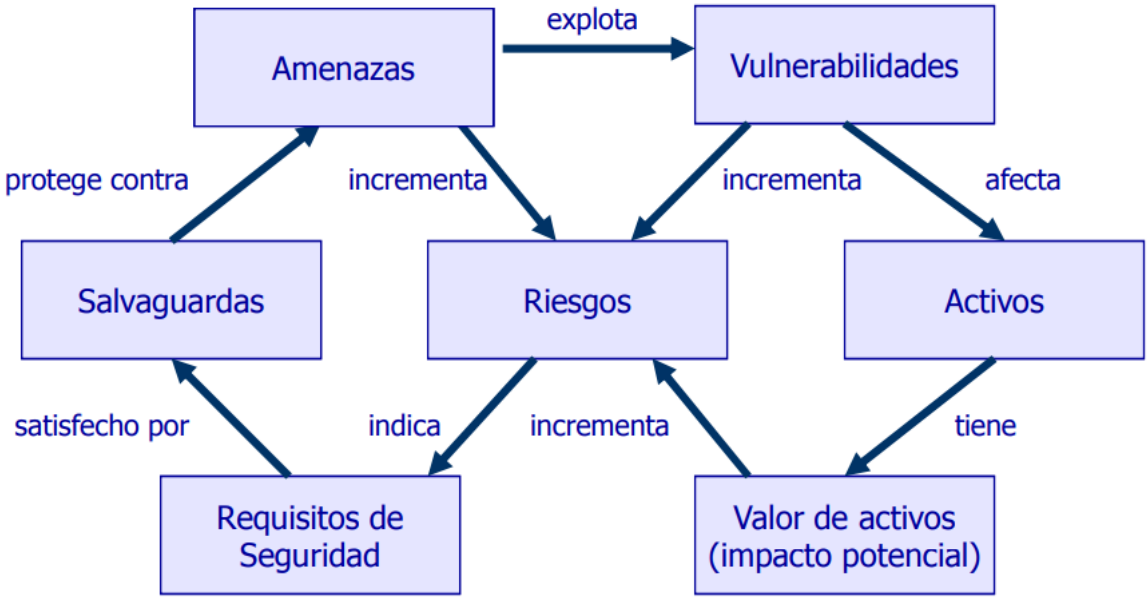


Figura 2. Elementos para análisis de riesgos.
Fuente: Recuperado de http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Como se puede observar en la Figura 2 existen varios elementos a tomar en cuenta para realizar un proceso de análisis de riesgos, destacando tres pilares fundamentales que son: salvaguardas, activos y amenazas. Para el cálculo oportuno de un valor de activos que representa un impacto potencial a la infraestructura.

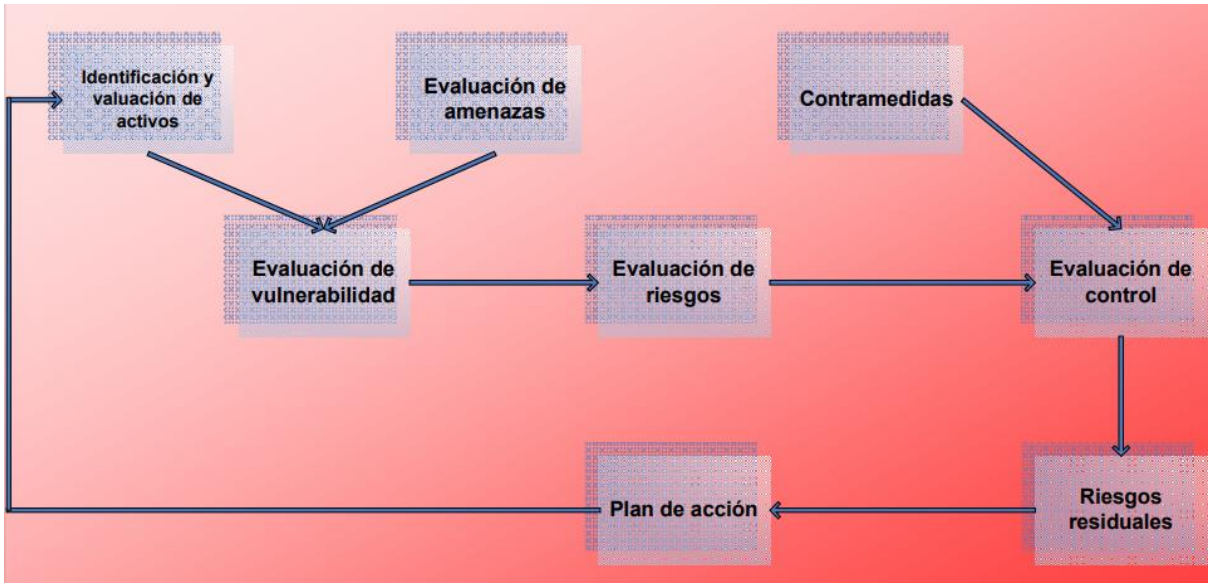


Figura 3. Proceso de análisis de riesgos
Fuente: IT Governance Institute

Para el proceso de elaboración de amenazas se identifican los activos las amenazas y de las cuales de puede destacar vulnerabilidades que afectan a los servicios y servidores implementados en una organización, con estos valores se puede obtener un estado inicial de la infraestructura.

En base al valor inicial de la organización o su estado de madurez se genera un plan de acción lo que puede derivar en implementación de políticas por medio de una normativa. Todo este proceso esta descrito en la Figura 3.

Existen varias metodologías de análisis de riesgos de las cuales se destacan las siguientes:

OCTAVE apunta a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. La tecnología es examinada en relación a las prácticas de seguridad, permitiendo a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica. El método OCTAVE permite la comprensión del manejo de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización. Exige llevar la evaluación de la organización y del personal de la tecnología de la información por parte del equipo de análisis mediante el apoyo de un patrocinador interesado en la seguridad. El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos:

- Identificación de la información a nivel gerencial.
- Identificación de la información a nivel operacional.
- Identificación de la información a nivel de usuario final.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información,

que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

2.1.2. Defensa en Profundidad

Se entiende cuando en un sistema se integran varias líneas de defensa continúas aumentando los niveles de protección, se puede intuir que el atacante al traspasar las protecciones perderá la intensidad en sus intentos y permitirá al administrador de la red mejorar y blindar la seguridad por etapas. Este conjunto de seguridades se puede observar en la Figura 4.

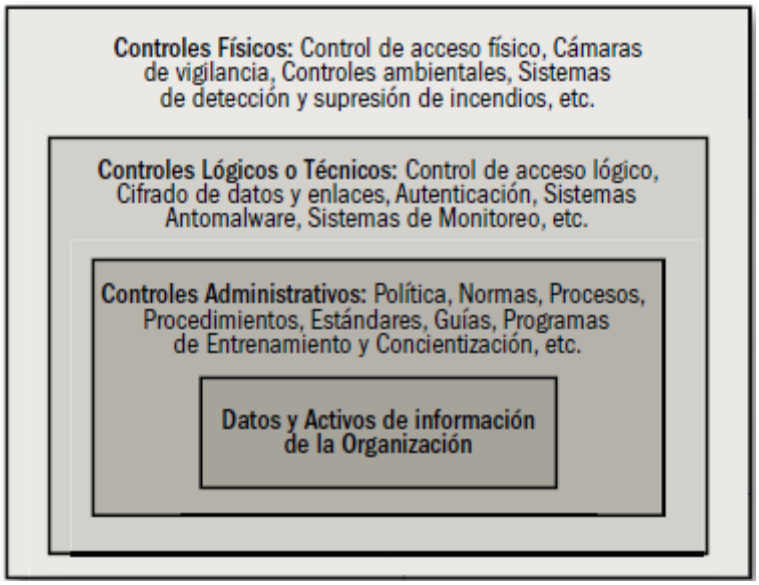


Figura 4. Representación de la defensa en profundidad.
Fuente: Elaborada por el autor

2.1.3. Fiabilidad

Hay que comprender que la seguridad de la información absoluta es un término imposible, por esta razón se utiliza el concepto de fiabilidad que representa la seguridad al máximo posible alcanzable mediante las técnicas de seguridad actuales. Para decir que un sistema es fiable se debe tomar en cuenta tres aspectos:

- Confidencialidad: Acceso a la información solo para los usuarios autorizados.
- Integridad: La información debe ser exacta y completa cuando se la requiera.
- Disponibilidad: Los usuarios autorizados deben tener acceso a los servicios cuando lo soliciten

2.1.4. Ataques Informáticos

En un comienzo los centros de datos se utilizaban por informáticos para realizar todo tipo de investigaciones y ataques lógicos a los equipos de manera controlada, con el avance de la tecnología y globalización del internet, surgieron personas que aplicaban sus conocimientos para sustraer información importante y además vulnerar sistemas, este tipo de sofisticadas técnicas se denominan ataques informáticos los cuales buscan aperturas en la seguridad de los sistemas de información, además de intentar obtener acceso a través de cualquier miembro de las organizaciones, por tal razón las organizaciones deben generar pruebas controladas de ataques informáticas y así dar con los errores antes que agentes externos a la organización.

En un ataque informático hay que analizar todo como un conjunto de etapas a realizar, generalmente en base a las siguientes fases se procede la mayoría de altercados o fallos en la seguridad:

- Fase 1 Reconocimiento: Consiste en conseguir información de acceso a un potencial objetivo sea este una persona u organización. Dentro de los métodos utilizados se pueden observar los siguientes:

- Fase 2 Escaneo: En esta etapa se utiliza los métodos anteriores para de esta manera conocer las características del sistema como direccionamiento, nombres y tipos de equipos, claves de acceso, etc.
- Fase 3 Obtener Acceso: En esta etapa se utilizan los procesos anteriores para explotar las vulnerabilidades del sistema.
- Fase 4 Mantener el Acceso: Al lograr el acceso es importante mantenerlo después mediante la implementación de puertas traseras y programas que permitan el acceso remoto mediante un acceso a internet.
- Fase 5 Borrar Huellas: Después se eliminará el rastro de acceso que se almacena en los logs o sistemas de alarma del sistema de seguridad implementado.

2.1.5. Debilidades comunes en seguridad:

Los mecanismos de seguridad se actualizan y suelen ser muy eficaces, pero es importante conocer las debilidades comunes que suelen ser explotadas de manera potencial por cualquier agente externo:

Ingeniería Social: Es un método que se aplica en todos los ámbitos consiste en aprovechar el factor humano de cualquier organización, haciendo uso del carisma o en otros caso de investigación de un factor humano vulnerable dentro de una organización para conseguir acceso a su información privada y de la empresa.

"Usted puede tener implementada la mejor tecnología, Firewalls, sistemas de detección de intrusos o complejos sistemas de autenticación biométricos... Pero lo único que se necesita es una llamada telefónica a un empleado desprevenido y acceden al sistema sin más. Tienen todo en sus manos" Kevin Mitnick, The Art of Intrusión.

- Códigos Maliciosos: Mejor conocidos como malware son programas que se introducen en un sistema por medio el usuario mediante usb, correo, aplicaciones,

etc. Suelen existir varios como troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.

- De los anteriores los más utilizados son los troyanos generalmente son archivos con un payload que debe ser ejecutado por el usuario que tiene instrucciones específicas para eliminar archivos o crear accesos remotos, capturas del teclado y funciones que atentan contra la seguridad de la información, al conseguir el acceso el atacante inserta rootkits o backdoors para mantener acceso remoto en toda ocasión.
- Contraseñas: Aunque en la actualidad no es muy recomendable su uso en la seguridad los atacantes siempre buscan acceder por medio de obtener un usuario y su contraseña mediante ataques de fuerza bruta, la debilidad viene dada por el factor humano ya que las contraseñas que una persona puede recordar no son complejas y se tiende a usar la misma contraseña para varios lugares como correo, redes sociales, aplicaciones interactivas, etc.
- Configuraciones por defecto: Se refiere a que la mayoría de administradores de red al implementar equipos y servidores por ahorrarse un poco de tiempo mantiene las configuraciones por defecto, lo que permite al atacante acceder por medio de telnet o ssh como usuario con privilegios.
- OSINT (Open Source Intelligence): Inteligencia de fuentes abiertas se refiere a que cada atacante realiza un proceso de investigación que parece complejo pero resulta ser muy simple, inician una exploración para recopilar información del objetivo por medio de lugares públicos de acceso es decir paginas públicas de información dentro de google o directamente por el navegador para de esta manera tener claro el ambiente con el que se enfrentara y las posibles vulnerabilidades e información que podría estar resguardando.

2.1.6. Pentesting

Sirve para evaluar los niveles de seguridad en un sistema informático o red de datos mediante un proceso de simulación controlad, que podría ser realizado por personas con conocimientos de informática denominados hacker.

La intención de este proceso es encontrar vulnerabilidades en los sistemas y servidores que se pueden encontrar por fallas en la configuración de seguridades por parte del administrador o encargado de un Data-Center, para su realización la persona encargada de realizar las pruebas de penetración se pone en la posición del atacante y realiza un informe detallado de los procesos realizados y las vulnerabilidades o fallos encontrados.

Tienen conjuntos de programas que permiten realizar estas pruebas de penetración las cuales facilitan la tarea y muchas veces se las puede obtener en un archivo ISO como sistema operativo ejecutable.

Fases del pentesting

Dentro de la realización de un test de intrusión se pueden ver diferentes fases o etapas, que se realizaran en un orden estructurado para resguardar la seguridad de los sistemas integrados, además se delimitara objetivos particulares y un objetivo general que es preservar la seguridad.

Estas fases de intrusión son las siguientes:

- Reglas del juego: Alcance y términos del test de intrusión
- Recolección de información
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades
- Postexplotación de vulnerabilidades
- Generación de informes

Reglas del juego: Alcance y términos del test de intrusión

Al inicio de cualquier auditoria es necesario definir los objetivos que se quiere alcanzar, el ámbito de acción, los peligros a los que está expuesta la organización al realizar la auditoria, además de las restricciones que impone el administrador o encargado de la red de datos.

Recolección de información

En esta etapa se recolecta toda la información concerniente al objetivo de ataque utilizando técnicas como Footprinnting, Fingerprinting, Google Hacking, entre otras.

Además, se utiliza ingeniería social con los trabajadores de la organización mediante revisión de sus redes sociales, todo este proceso permite al auditor tener un panorama completo en base a los objetivos planteados.

Análisis de vulnerabilidades

Una vez recolectada toda la información se realiza un informe de todas las vulnerabilidades posibles encontradas, mediante el cual se empezará a planificar el método de acción que mejor se adapte a la infraestructura.

Explotación de vulnerabilidades

En esta etapa se procede a realizar las pruebas de intrusión delimitadas posteriormente en el plan de acción, la mayoría de auditores por economizar tiempo proceden a la utilización de exploits, lo cual no es recomendable porque a veces se realiza mucho daño en el sistema, por este motivo es mejor seguir procesos estandarizados de manera manual que permitan observar las vulnerabilidades de manera organizada.

Postexplotación

En esta etapa ya se posee el control de un equipo en la red de datos, pero el atacante no se detendrá, intentara tomar el control de todos los equipos para obtener información delicada, el auditor tiene como responsabilidad pensar como lo hace un atacante es decir pensar el alcance que un atacante le podría dar a este acceso.

Generación de informes

Esta etapa es la documentación de todo el proceso realizado y las vulnerabilidades encontradas, sirve como una guía en caso de necesitar la realización de un plan de contingencia y mejora.

2.1.6.1.Kali-Linux

Es una reestructuración completa de BackTrack 5, pero en lugar de desarrollarse sobre Ubuntu, este sistema operativo está construido sobre las bases de Debian aumentando su compatibilidad con 300 herramientas más de pentesting.

Las características destacables de Kali-Linux son:

- Soporte para dispositivos inalámbricos
- Se utiliza Git como software para el desarrollo y construcción de soluciones de las distintas herramientas.
- Todas las herramientas son de código abierto, permitiendo su modificación o personalización.
- Las herramientas están desarrolladas en varios idiomas para mejorar su interacción.
- Sus paquetes están disponibles en los repositorios de Debian.
- Su interfaz se puede modificar según la comodidad del usuario.
- El sistema es código abierto y totalmente gratuito.

Se puede utilizar este software para auditorías internas, externas y web, mediante una cantidad enorme de herramientas dedicadas para cada una de las tareas, que permiten realizar pruebas de intrusión y búsqueda de vulnerabilidades para útiles en todo tipo de organización.

2.1.7. Medidas de Control

Hay que tener en consideración que ningún sistema es totalmente seguro, pero mediante cierto tipo de acciones y medidas se puede mantener una relativa seguridad controlada, existen varias maneras de mejorar los niveles de seguridad:

2.1.7.1.Seguridad perimetral

La globalización de la internet y el acceso a todo tipo de información de parte del usuario, permite que el sistema de información se convierta en un ente vulnerable a todo tipo de amenazas que pueden perjudicar a la confidencialidad, disponibilidad, integridad del sistema o equipos que lo conformen que contengan en sus bases de datos información de sus servicios y usuarios.

La seguridad perimetral confiere a la organización métodos para asegurar su red basado en nieles de acceso por usuario y servicio sea de forma externa o interna, se enfoca en sectores de la organización según el tipo de información, su objetivo es proteger los sistemas de información de manera estructurada y focalizada según el perímetro, prioridad y la importancia de los datos almacenados.

Es la integración de sistemas y elementos para la protección de perímetros internos y externos, además detecta, disuade y frena al intruso con mucha más antelación.

Estos elementos son:

- Proxy
- Honeypot
- Cortafuegos (firewall)

2.1.7.1.1. Proxy

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo, se encarga de redirigir el tráfico de acceso mediante un puerto seguro que se encarga de descartar peticiones no autorizadas y bloquear sitios almacenados en sus black list, además de regular el tráfico de datos y generar prioridad según sectores de red o usuario con niveles de acceso y tiempos de uso.

2.1.7.1.2. Honeypot

Es un sistema operativo que se encarga de simular un servidor con la mayoría de puertos y servicios vulnerables para atraer los atacantes, una vez que el atacante accede toda la información y procedimiento realizado se almacena en sus logs privados ayudando al administrador de la red a prevenir las fallas en base al procedimiento realizado por el agente externo.

Dos tipos principales de honeypots:

- **De baja interacción:** aplicación que simula vulnerabilidad y sistema operativo.
- **De alta interacción:** el sistema operativo no es simulado.

2.1.7.1.3. Cortafuegos (firewall)

El firewall se ha convertido en un dispositivo indispensable dentro de cualquier arquitectura de red, servidores que tengan acceso a Internet. Estos dones dispositivos o sistemas que controlan el tráfico de la red, en las cual aplica ciertas políticas de seguridad, la complejidad de estos se basa en las reglas que admiten o bloquean los accesos.

El cortafuego va interactuando en cada una de las capas del modelo OSI como se observa en la Figura 5.

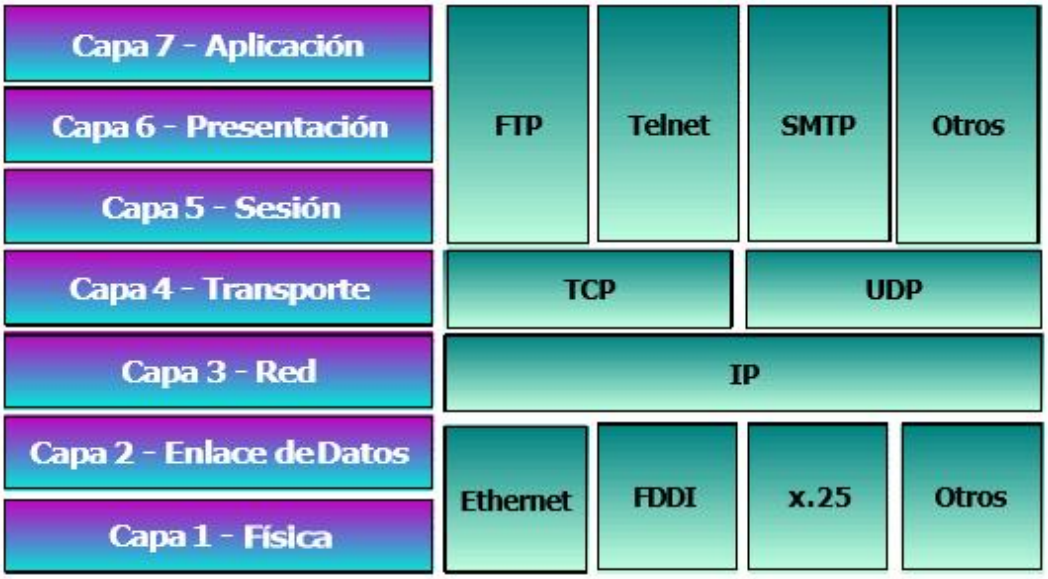


Figura 5. Servicios de protocolos más usados en las capas del modelo
Rescatado de: http://www.moratalaz.jazztel.es/pdfs/cortafuegos.pdf

Los cortafuegos se dividen en dos tipos:

- Cortafuegos a nivel de red. - trabaja en la capa 2,3 y 4 del modelo OSI.
- Cortafuegos a nivel aplicación. - trabajan en la capa 5,6 y 7 del modelo OSI

Cortafuegos a nivel de red

Se encarga de la administración de la seguridad de las direcciones físicas (MAC), lógicas (IP), los puertos de comunicación y protocolos, es importante denotar que esta seguridad se la aplica de manera perimetral al sistema de red y procesa todas las peticiones de los usuarios mediante aplicaciones al internet e intranet.

Cortafuegos a nivel aplicación

Se lo denomina antivirus y su principal función es la de proteger al equipo de interacción con el usuario y las solicitudes de red, resguarda la funcionalidad del sistema operativo y los archivos personales y datos de acceso del cliente.

Ventajas

- Restricción de accesos no deseados a una red
- Creación de reglas de entrada o salida en una red
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.
- Protección de los datos. Base de datos de los usuarios de la red
- Técnica para abordar las amenazas de seguridad en evolución

Limitaciones

- El firewall no puede prohibir que se copien datos corporativos en disquetes o memorias portátiles y que estas se substraigan del edificio.
- Un cortafuego o firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- El cortafuegos no puede proteger contra los ataques de “Ingeniería Social”
- El cortafuego no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a internet.

Capitulo III

Situación Actual

Para cumplir con los requerimientos del desarrollo e implementación de un SGSI es necesario detallar las condiciones actuales de los equipos integrados en el Data-Center, la documentación de las políticas, responsabilidades de los encargados, las características físicas de los servidores y los servicios presentes en la infraestructura.

La Universidad Técnica del Norte en su infraestructura cuenta con un Data-Center principal ubicado en el edificio central, conformado por varios equipos de red, y servidores entre los que se puede destacar el servidor de telefonía IP, servidor web, servidor DHCP, Firewall CISCO ASA 5520, y el switch core primario y secundario (respaldo) que comunica con cada facultad además de las dependencias externas por medio de enlaces inalámbricos. La topología física general de la Universidad Técnica del Norte la podemos observar en la Figura 6.

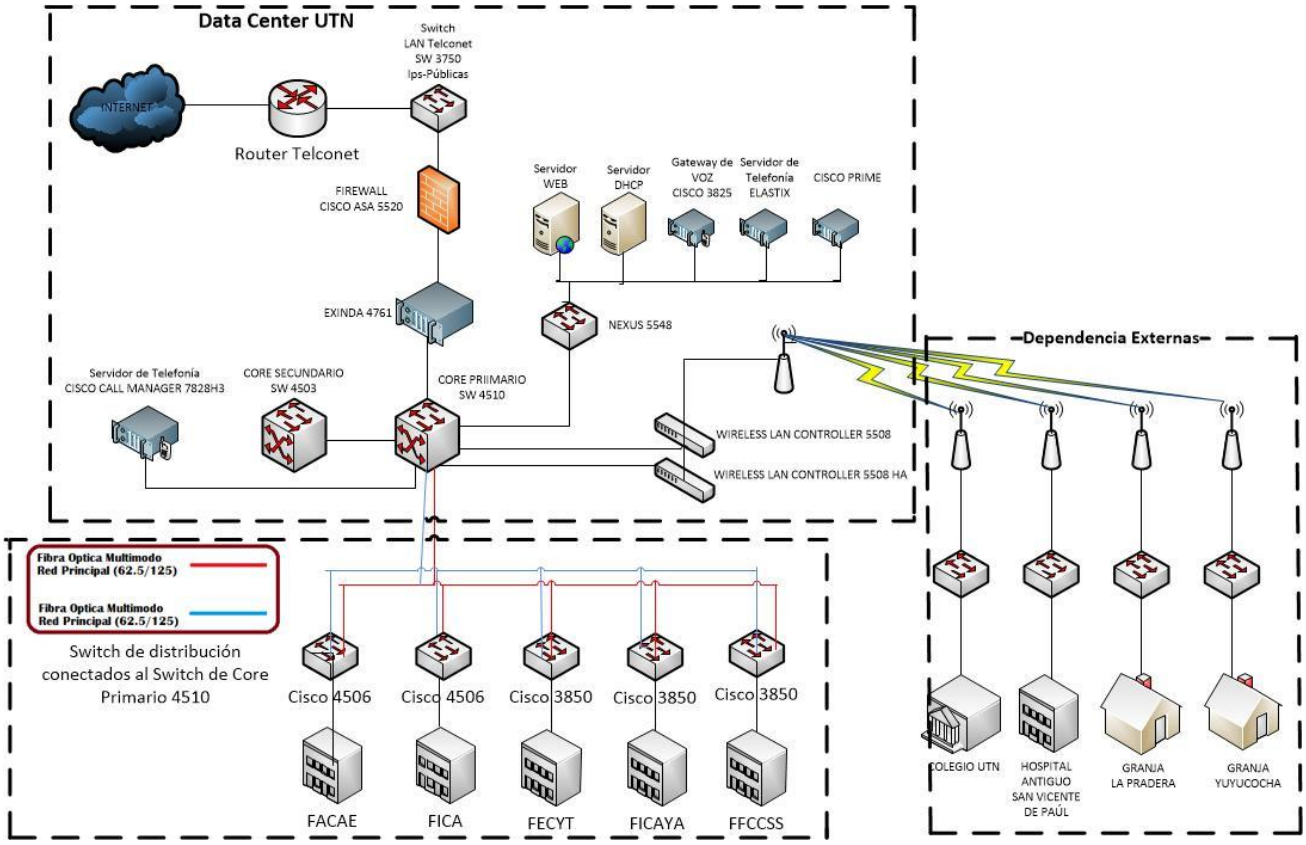


Figura 6.Figura. Diagrama Físico UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

3.1. Topología FICA

Para delimitar el alcance del proyecto es indispensable realizar una topología tanto física como lógica que permita delimitar el campo de acción.

3.1.1. Topología Física

En la facultad de ingeniería y ciencias aplicadas de la universidad técnica del norte se realizó la implementación de un Data-Center para ubicación de equipos de red encargados de la interconexión de los laboratorios y el centro de datos del edificio central y su posterior enlace con la red externa o Internet, además de los servidores integrados. La topología Física se observa en la Figura 7.

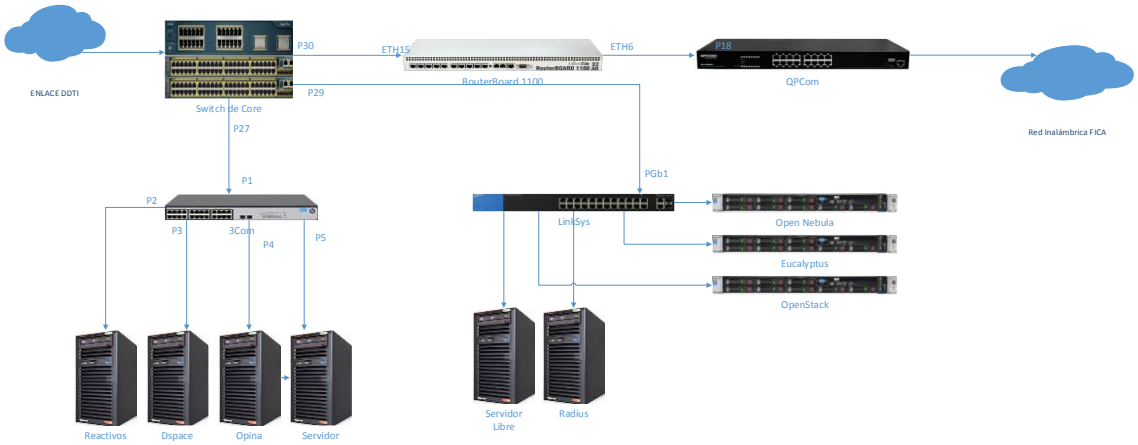


Figura 7. Topología Data-Center
Fuente: Centro de Datos FICA

Como se puede observar en la Figura 5 el acceso a internet esta proporcionado por un enlace de fibra óptica desde el DDTI hasta el switch de core.

La red inalámbrica FICA está conectada por medio de un cable utp categoría 5E desde el puerto 30 del switch de core hasta el puerto ETH15 del Switch de capa 3 administrable de marca Mikrotik, el cual se encarga de realizar un bridge de acceso hacia el puerto ETH6 que se interconecta con el Switch de capa 2 QPCOM, el cual por medio de una conexión en su puerto 18 se encarga de replicar el enlace proporcionado por el Mikrotik a los distintos Access point ubicados en la Facultad.

El sistema de servidores cloud está conectado desde el switch de Core por medio del puerto 29 del catalyst hacia el puerto Gibabit Ethernet 1 del switch linksys que a su vez replica la conexión recibida hacia cada uno de los servidores que se encuentran conectados al mismo, los cuales son: eucaliptus; openstack; open nebula, como servidores de virtualización y a dos servidores de torre los cuales se pueden definir como: SDN que se encuentra fuera de funcionamiento; un servidor radius que trabaja para negociación de acceso a la red inalámbrica, además se manejan dos puertos del switch antes mencionado para la conexión de los sensores de temperatura implementados en los paneles del rack.

Por último, se debe destacar un enlace desde el switch de core en el puerto 27 que se enlaza con un switch 3com, el que se encuentra replicando la conexión hacia 4 servidores de torre los cuales son: servidor de reactivos de la facultad, servidor de los paneles de acceso biométrico, servidor opina y el servidor Dspace.

El posicionamiento físico de los equipos en base a los 3 rack que se encuentran en el Data-Center viene representado por la Figura 8.

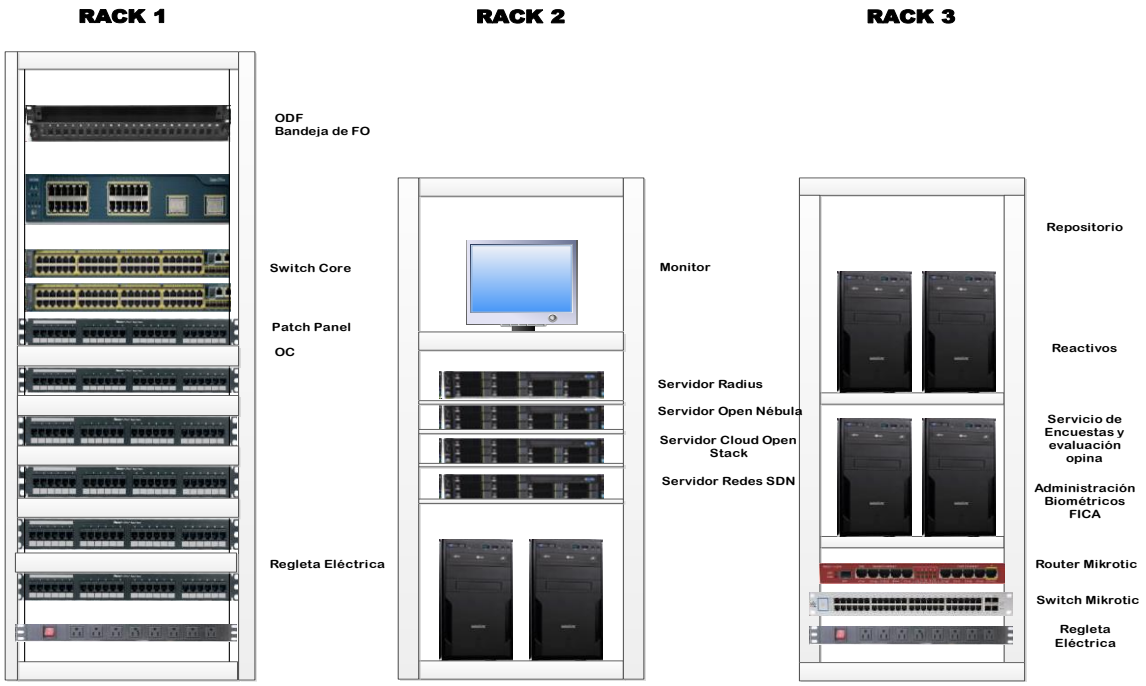


Figura 8. Ubicación Física equipos Data-Center
Fuente: Data-Center FICA

3.1.2. Topología Lógica

La distribución a nivel lógico de los servidores es uno de los procesos fundamentales al momento de recopilar la información, debido a que la idea central de este proceso es realizar una adaptación menos intrusiva posible e intentar utilizar el direccionamiento o red lógica implementada, solo se procede a su modificación en caso de encontrar deficiencias que lo ameriten.

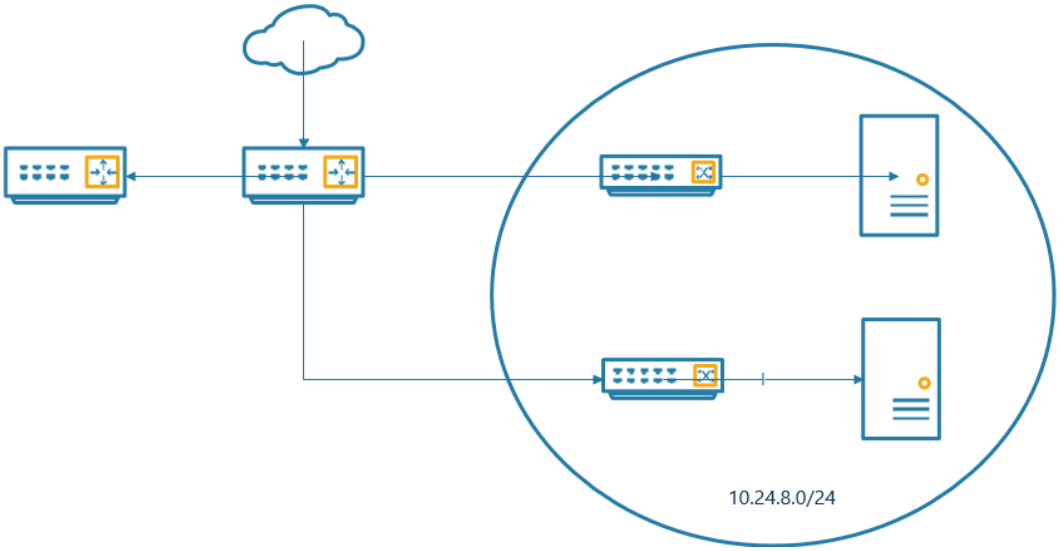


Figura 9. Topología lógica
Fuente: Realizado por el autor

Como se puede observar en la Figura 9, la red es plana con un solo rango de direcciones para los servidores destinados cloud ubicados en el rack 2 y los servidores de torre ubicados en el rack 3, además la red inalámbrica es independiente de los servicios integrados en el Data-Center.

3.2. Estructura Organizacional del Data-Center

En la investigación realizada se puede destacar que el Data-Center cuenta con una estructura organizacional descentralizada, por lo cual existe una persona a cargo denominada administrador de red, y el resto de servidores cuenta con un encargado o responsable, que se encarga del mantenimiento independiente de cada servidor.

Los equipos se encuentran asignados de manera independiente por cada docente a cargo del proyecto como se muestra en la Tabla 3.

Tabla 3.
Características de los equipos y los responsables a cargo

Modelo	Ubicación	Función o Uso	Encargado
IBM System x 3200 M2	Rack 2	Radius	Ing. Hernan Dominguez
ProLiant DL360 Gen 9	Rack 2	Servidor Open Nebula	Ing. Edgar Jaramillo
HP Proliant DL 150 G9	Rack 2	Redes SDN	Ing. Edgar Jaramillo
HP Proliant DL 360 G9	RACK 3	Servidor Cloud Open Stack	Ing. Edgar Jaramillo
HP Proliant ML 150 G5	RACK 3	Servicio de encuestas y evaluación Opina	Ing. Edgar Jaramillo
IBM System x3500 M4	RACK 3	Reactivos	Ing. Fernando Garrido
IBM System x3500 M4	RACK 3	Repositorio o DSpace	Ing. Fernando Garrido
PC tipo “CLON” H81M-S1		Administración biométricos FICA	Ing. Carlos Vásquez

Fuente: Creado por el autor

3.2.1. Políticas de Seguridad

De la recopilación de la información podemos destacar que existen políticas implementadas dentro del Data-Center las cuales se encuentran recopiladas en el Anexo 3.

Además, se encontraron los siguientes manuales de procedimiento el primero para el ingreso de personas al Data-Center que se puede encontrar en el Anexo 4 y el segundo para Entrada/Salida de equipos del Data-Center disponible en el Anexo 6.

3.2.1.1. Formatos

Se encuentran disponibles los siguientes formatos respectivamente:

- Entrada/Salida de equipamiento en el Centro de Datos FICA (Anexo 6)
- Solicitud de ingreso al Centro de Datos FICA (Anexo 7)

- Control de ingreso de Personas al Centro de Datos FICA (Anexo 4)

3.3. Equipos Servidores

Cada uno de los servidores integrados en el Data-Center posee ciertas características que interesa destacar en base a su aplicación y por lo cual permite delimitar el campo de acción para el diseño de la solución propuesta.

3.3.1. Detalles Técnicos

Los servidores cuentan con características específicas que permiten realizar un diagnóstico rápido en caso de producirse un incidente.

Dentro del Anexo 2 se encuentra detallado cada equipo servidor con sus características de hardware que sirven para delimitar sus capacidades y posibles funcionalidades.

3.4. Análisis de riesgos

Para la determinación de los riesgos presentes en el Data-Center se realizará un proceso en base a la metodología de análisis y gestión de riesgos de los sistemas de información por sus siglas MAGERIT, el cual es un modelo libre y orientado a la administración pública por lo que permite su utilización para el entorno actual.

Dentro de la metodología se comprende la estructura de análisis de riesgo en base a las siguientes definiciones y clasificaciones de los equipos que integran un sistema de gestión de la información que son:

- Determinar los activos relevantes para la organización, su interacción y su valor, en el sentido del perjuicio supondrá su degradación. (Amutio Gomez, 2012)
- Determinar a qué amenazas están expuestos aquellos activos. (Amutio Gomez, 2012)

- Determinar a qué salvaguardas hay dispuestas y que tan eficaces son frente al tipo de riesgo. (Amutio Gomez, 2012)
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza. (Amutio Gomez, 2012)
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de la amenaza. (Amutio Gomez, 2012)

Método de análisis de riesgos

Se debe destacar que la información recolectada en la situación actual del Data-Center es un punto de inicio para la elaboración de las matrices de riesgos, dentro de la valoración del entorno inicial de esta metodología que sostiene como procesos estandarizados lo siguiente:

- Facilitar la labor de las personas mediante una estandarización del sistema objeto de análisis.
- Homogeneizar los resultados de los análisis, para comparar distintos equipos presentes en la infraestructura.

El proceso de categorización de los componentes de una organización está definido en el libro II de MAGERIT, y contempla lo siguiente para estructurar el análisis y la matriz de riesgos:

- Activos
- Amenazas
- Salvaguardas

Dentro de los activos se procederá a especificar cada uno de ellos, esta caracterización se encuentra descrita a continuación.

Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberadamente o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (Software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y humanos. (UNE 71504:2008, 2008)

Activos Esenciales: La importancia de un activo es la información que maneja y los servicios que prestan, dentro de la definición para su clasificación hay que destacar los equipos del Data-Center que entran en esta clasificación según MAGERIT están representados en la Tabla 4.

Tabla 4.
Activos esenciales del Data-Center

Activos Esenciales										
Equipo	**Información [info]**		**Datos Personales [per]**			**Datos Clasificados [classified]**				**Servicios [service]**
	[adm]	**[vr]**	**[A]**	**[M]**	**[B]**	**[C]**	**[R]**	**[UC]**	**[pub]**	
IBM Systemx3200 M2 (Radius)										X
HP Proliant DL360 G9 (Openstack)				X			X			X
HP Proliant ML150 G5 (Opina)			X				X			X
IBM Systemx3500 M4 (Reactivos o moodle)			X			X	X			X
IBM Systemx3500 M4 (DSpace)	X						X			X
PC tipo Clon H8M-S1		X				X				X

Fuente: Elaborada por el autor. [info]: información, [adm]: datos de interés para la administración pública, [vr]: registros de la organización, [per]: datos de carácter personal, [classified]: datos clasificados, [A]: nivel alto, [M]: nivel medio, [B]: nivel bajo, [service]: servicio, [C]: nivel confidencial, [R]: difusión limitada, [UC]: sin clasificar, [pub]: publico..

Arquitectura del sistema: Son los elementos que permiten estructurar el sistema definiendo arquitectura interna, los equipos disponibles dentro del Data-Center que entran en la clasificación están descritos en la Tabla 5.

Tabla 5.
Activos de Arquitectura del sistema del Data-Center

Arquitectura del Sistema			
Equipo	**Punto de Acceso al Servicio [sap]**	**Punto de interconexión [ip]**	**Proporcionado por terceros [ext]**
Switch de Core Catalyst 4506-E	X		X
RouterBoard 1100 Mikrotik	X	X	
Switch de Distribución 3Com		X	
Switch de Distribución Linsys		X	
Switch Distribución inalámbrica QPCOM		X	

Fuente: Elaborada por el autor. [sap]: punto de acceso al servicio, [ip]: punto de interconexión, [ext]: proporcionado por terceros.

Por sus características desglosadas se puede subdividir a los activos en base a 4 parámetros que abarcan o afectan a las funcionalidades lógicas de los activos presentados en la Tabla 4 y Tabla 5, esta clasificación viene dada por lo siguiente:

Datos / Información: Los datos son la parte esencial de una organización, esta se almacena en equipos o serán transferidos por medios de transmisión. Dentro de este apartado existen equipos que almacenan información y serán descritos en la Tabla 6.

Tabla 6.
Equipos Datos / Información del Data-Center FICA

Datos / Información								
Equipo	**Fichero[files]**	**Respaldos [backup]**	**Datos de configuración [conf]**	**Datos de gestión interna [int]**	**Contraseñas [password]**	**Datos de control de acceso [acl]**	**Registro de actividad [log]**	**Código Fuente [source]**
IBM Systemx3200 M2 (Radius)	X		X	X	X	X	X	X
HP Proliant DL360 G9 (Openstack)	X		X	X	X	X	X	X
HP Proliant ML150 G5 (Opina)	X						X	X
IBM Systemx3500 M4 (Reactivos o moodle)	X	X			X	X	X	X
IBM Systemx3500 M4 (DSpace)	X						X	X
PC tipo Clon H8M-S1 (Biométricos)					X	X	X	X

Fuente: Elaborada por el autor. [files]: ficheros, [backup]: copias de respaldo, [conf]: datos de configuración, [int]: datos de gestión interna, [password]: credenciales, [acl]: datos de control de acceso, [log]: registro de actividad, [source]: código fuente.

Servicios: Es una función que satisface las necesidades de los usuarios, en la Tabla 7 se encuentran los equipos del Data-Center que cumplen con el objetivo de brindar un servicio a usuarios finales.

Tabla 7.
Equipos Datos / Información del Data-Center FICA

	Servicios									
Equipo	**Anónimo [anon]**	**Público [pub]**	**Usuarios externos [ext]**	**Internos [int]**	**Worl wide web [www]**	**Correo electrónico [email]**	**Almacenamiento de ficheros [file]**	**Transferencia de archivos [ftp]**	**Gestion de identidades [idm]**	**Servicio de directorio [dir]**
IBM Systemx3200 M2 (Radius)			X	X	X					
HP Proliant DL360 G9 (Openstack)		X	X	X	X	X	X	X		X
HP Proliant ML150 G5 (Opina)	X		X	X			X			
IBM Systemx3500 M4 (Reactivos o moodle)				X	X	X		X		X
IBM Systemx3500 M4 (DSpace)				X				X		
PC tipo Clon H8M-S1 (Biométricos)				X					X	

Fuente: Elaborada por el autor. [anon]: anónimo, [pub]: público en general, [ext]: usuarios externos, [int]: interno, [www]: world wide web, [email]: correo electrónico, [file]: almacenamiento de ficheros, [ftp]: transferencia de ficheros, [ftp]: transferencia de ficheros, [dir]: servicio de directorio.

Software-Aplicaciones informáticas: Se denominan programas, aplicativos, etc. Pero este apartado se centra en los sistemas que permiten interactuar con el usuario final y brindar una plataforma que permita obtener información y brindar soluciones de manera lógica. En la Tabla 8 se puede observar los equipos del Data-Center que entran en esta clasificación.

Tabla 8.
Equipos con software o aplicaciones informáticas del Data-Center FICA

Software o Aplicaciones informáticas								
Equipo	**Desarrollo propio [prp]**	**Navegador web [browser]**	**Servidor de aplicaciones [app]**	**Servidor de correo electrónico [email_server]**	**Base de datos [dbms]**	**Monitor Transaccional [tm]**	**Gestor máquinas virtuales [hypervisor]**	**Sistemas de backup [backup]**
IBM Systemx3200 M2 (Radius)					X	X		
HP Proliant DL360 G9 (Openstack)		X	X				X	
HP Proliant ML150 G5 (Opina)		X	X					
IBM Systemx3500 M4 (Reactivos o moodle)		X	X	X	X			
IBM Systemx3500 M4 (DSpace)					X			
PC tipo Clon H8M-S1 (Biométricos)					X			

Fuente: Elaborada por el autor. [prp]: desarrollo propio, [browser]: navegador web, [app]: servidor de aplicaciones, [email_server]: servidor de correo electrónico, [dbms]: sistema de gestión de base de datos, [tm]: monitor transaccional, [hypervisor]: gestor de máquinas virtuales, [backup]: sistema de backup.

Equipamiento informático (HW): Son los materiales físicos destinados a soportar directa o indirectamente los servicios que brinda la organización, los equipos que cumplen con esta clasificación están descritos en la Tabla 9.

Tabla 9.
Equipamiento informático (Hardware) del Data-Center FICA

Equipamiento informático							
Equipo	**Grandes equipos [host]**	**Equipos medios [mid]**	**Equipo virtual [vhost]**	**Equipo de respaldo [backup]**	**Dispositivos de frontera [bp]**	**Concentradores [hub]**	**Conmutadores [switch]**
IBM Systemx3200 M2 (Radius)	X						
HP Proliant DL360 G9 (Openstack)	X		X				
HP Proliant ML150 G5 (Opina)	X						
IBM Systemx3500 M4 (Reactivos o moodle)	X			X			
IBM Systemx3500 M4 (DSpace)	X						

PC tipo Clon H8M-S1 (Biométricos)	X			
Switch de Core Catalyst 4506-E			X	
RouterBoard 1100 Mikrotik				X
Switch de Distribución 3Com			X	
Switch de Distribución Linsys			X	
Switch Distribución inalámbrica QPCOM			X	

Fuente: Elaborada por el autor. [host]: grandes equipos, [mid]: equipos medios, [vhost]: equipo virtual, [backup]: equipamiento de respaldo, [bp]: dispositivos de frontera, [hub]: concentradores, [switch]: conmutadores.

Todas las notaciones, los parámetros de clasificación de activos se encuentran referenciadas en el Anexo 9, Es importante destacar que los activos tienen varias características contempladas en MAGERIT, la Tabla 10 indica la clasificación general de cada activo que integra el Data-Center.

Tabla 10.
Clasificación General de Equipos del Data-Center FICA

Equipo	**Clasificación**			
	Datos / Información [di]	**Servicios [S]**	**Sotware- Aplicaciones informáticas [SW]**	**Equipos Informáticos [HW]**
IBM Systemx3200 M2 (Radius)	X	X	X	X
HP Proliant DL360 G9 (Openstack)	X	X	X	X
HP Proliant ML150 G5 (Opina)	X	X	X	X
IBM Systemx3500 M4 (Reactivos o moodle)	X	X	X	X
IBM Systemx3500 M4 (DSpace)	X	X	X	X
PC tipo Clon H8M-S1 (Biométricos)	X	X	X	X
Switch de Core Catalyst 4506-E				X
RouterBoard 1100 Mikrotik		X	X	X
Switch de Distribución 3Com				X
Switch de Distribución Linsys				X
Switch Distribución inalámbrica QPCOM				X

Fuente: Elaborada por el autor. [di]: datos e información, [S]: Servicios, [SW]: Software- aplicaciones informáticas, [HW]: Equipos informáticos..

Valoración de los Activos:

Para la valoración de los activos se tomará en cuenta la triada de la informática que son Disponibilidad, Integridad y Confiabilidad. Dentro de los parámetros se descarta trazabilidad y autenticidad porque se encuentran incluidos, se generará una estadística independiente por activo que dará a conocer el valor que tiene para la organización, según MAGERIT es importante generar una escala que se encuentra representada en la Tabla 11.

Tabla 11.
Valor del Activo/Criterio

Valor	Criterio
1	Muy Bajo
2	Bajo
3	Medio
4	Alto

Fuente: Recuperado de MAGERIT versión 3.0 Libro II – Catalogo de Elementos

Disponibilidad: Para la asignación de este valor se realiza la pregunta de cuál sería la afectación al centro de datos ocasionaría si el activo no está disponible, para lo cual se puede usar como indicadores lo descrito en la Tabla 12.

Tabla 12.
Valor del Activo según la disponibilidad

Valor	Criterio
1	No Aplica/No es relevante
2	Debe estar disponible al menos el 10%
3	Debe estar disponible al menos el 50%
4	Debe estar disponible al menos el 99%

Fuente: realizado por el autor

Integridad: Para encontrar este valor la pregunta qué importancia tendría el activo si es alterado sin autorización ni control, En la Tabla 13 se encuentra la valoración y el criterio establecido.

Tabla 13.
Valor del Activo según la integridad

Valor	Criterio
1	No Aplica/No es relevante
2	No es relevante los errores que tenga o la información que falte
3	Tiene que estar correcto y completo al menos en un 50%
4	Tiene que estar correcto y completo al menos en un 95%

Fuente: realizado por el autor

Confidencialidad: En esta situación la pregunta a responder es cuál es la importancia que tendría al activo un acceso no autorizado, para esto se utiliza la Tabla 14.

Tabla 14.
Valor del Activo según la confiabilidad

Valor	Criterio
1	No Aplica/No es relevante
2	Daños muy bajos, el incidente no trascendería del área afectada
3	Serian relevantes, el incidente implicaría a otras áreas
4	Los daños serian catastróficos, la reputación y la imagen de la organización se verían comprometidas

Fuente: realizado por el autor

De la información descrita en las tablas anteriores se puede realizar una valoración de cada uno de los activos en base a los tres parámetros descritos y los activos que se encuentran en la infraestructura. Esta recopilación se encuentra en la Tabla 15.

Tabla 15.
Valor del Total del activo

Equipo	Valorización			Magnitud del daño
	Disponibilidad	Integridad	Confiabilidad	
IBM Systemx3200 M2 (Radius)	4	3	2	3
HP Proliant DL360 G9 (Openstack)	3	4	4	3,6
HP Proliant ML150 G5 (Opina)	4	4	4	4
IBM Systemx3500 M4 (Reactivos o moodle)	4	4	4	4
IBM Systemx3500 M4 (DSpace)	3	3	3	3
PC tipo Clon H8M-S1 (Biométricos)	4	3	3	3,3
Switch de Core Catalyst 4506-E	4	2	3	3
RouterBoard 1100 Mikrotik	4	2	2	2,6
Switch de Distribución 3Com	2	1	1	1,3
Switch de Distribución Linsys	2	1	1	1,3
Switch Distribución inalámbrica QPCOM	3	1	1	1,6

Fuente: realizado por el autor

De la Tabla 15 se puede observar los valores de los activos por medio de un promedio de los tres parámetros se procede a realizar el cálculo del valor total del activo, en caso de tener valores decimales se aproximará al inmediato superior. Para la obtención de estos parámetros se tomo en cuenta el libro II de MAGERIT catalogo de elementos de donde se procede a realizar una valoración en base a la información que maneja cada uno de los activos, lo que se puede encontrar en el Anexo 9.

Hay que destacar que por ser la primera vez que se realiza un análisis de riesgos para la infraestructura lo que se obtendrá es el estado inicial de la organización y de los activos existentes.

Amenazas

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (UNE 71504:2008, 2008).

Las amenazas que se pueden encontrar en un sistema de información están contempladas en la metodología MAGERIT en su libro II y reseñadas en el Anexo 10.

En la Tabla 16 se puede observar el desglose de todas las amenazas según los tipos de activos, y la incidencia que tienen en la triada informática que son confidencialidad, integridad y disponibilidad.

Tabla 16.
Tabla de amenazas del Data-Center

Amenaza		Tipos de Activos											
		Datos / Información [di]			Servicios [S]			Software- Aplicaciones informáticas [SW]			Equipos Informáticos [HW]		
Cod	**Des**	D	I	C	D	I	C	D	I	C	D	I	C
Origen Natural													
N.1	Fuego										X		
N.2	Daños por agua										X		
N.*	Desastres Naturales										X		
Origen Industrial													
L.1	Fuego										X		
L.2	Daños por agua										X		
L.*	Desastres industriales										X		
L.3	Contaminación mecánica										X		
L.4	Contaminación electromagnética										X		
L.5	Avería Fisca/Lógica										X		
L.6	Corte eléctrico										X		
L.7	Condiciones inadecuadas										X		
L8	Fallo servicios comunicación										X		
L.9	Interrupción servicios										X		
L.10	Degradación soportes almacenamiento										X		
L.11	Emanaciones electromagnéticas												X
Origen Humano (Accidental)													
E.1	Errores de los usuarios	X	X	X	X	X	X	X	X	X			
E.2	Errores del administrador	X	X	X	X	X	X	X	X	X	X	X	X
E.3	Errores de monitorización		X			X							
E.4	Errores de configuración		X			X							
E.8	Difusión de software dañino							X	X	X			
E.9	Errores de encaminamiento				X	X	X	X	X	X			
E.10	Errores de secuencia								X				

E.14	Escapes de información			X									
E.15	Alteración accidental de la información		X			X			X				
E.18	Destrucción de la información	X			X			X					
E.19	Fugas de información			X			X			X			
E.20	Vulnerabilidades de los programas							X	X	X			
E.21	Errores de mantenimiento/actualización de programas							X	X				
E.23	Errores de mantenimiento/actualización de equipos										X		
E.24	Caída del sistema por agotamiento de recursos				X						X		
E.25	Perdida de equipos										X		X
Origen Humano (Deliberado)													
A.3	Manipulación de los registros de actividad		X										
A.4	Manipulación de la configuración	X	X	X									
A.5	Suplantación de la identidad del usuario		X	X		X	X		X	X			
A.6	Abuso de privilegios de acceso	X	X	X	X	X	X	X	X	X	X	X	X
A.7	Uso no previsto				X	X	X	X	X	X	X	X	X
A.8	Difusión de software dañino							X	X	X			
A.9	Re-encaminamiento de mensajes						X			X			
A.10	Alteración de secuencia					X			X				
A.11	Acceso no autorizado		X	X		X	X		X	X		X	X
A.13	Repudio					X							
A.15	Modificación deliberada de la información		X			X			X				
A.18	Destrucción de la información	X			X			X					
A.19	Divulgación de información			X			X			X			
A.22	Manipulación de programas							X	X	X			
A.23	Manipulación de los equipos										X		X
A.24	Denegación de servicio				X						X		
A.25	Robo										X		X
A.26	Ataque destructivo										X		

Fuente: Basado en MAGERIT

Salvaguardas

El Data-Center cuenta con las salvaguardas que se encargaran de proteger a los equipos de las amenazas al hardware, dentro de las cuales se debe destacar las siguientes:

- Control de acceso biométrico: Solo el personal autorizado puede acceder al Data-Center
- Sistema de alimentación ininterrumpida: En caso de fallos o desconexión del sistema eléctrico principal, se encarga de brindar respaldo y mantener operativos los activos que integran el Data-Center
- Sistema de control de temperatura: Existe una infraestructura formada por sensores y sistemas de alerta que permiten controlar que la temperatura se mantenga en rangos adecuados de funcionamiento, así como un equipo de enfriamiento.

Dentro de la parte lógica de la red el Data-Center solo posee una salvaguarda para control de accesos a la red inalámbrica de los estudiantes que integran la FICA, el cual consta de dos equipos que interactúan entre sí:

- RouterBoard 1100 Mikrotik
- Servidor Radius

Estos dos equipos complementan todas las seguridades lógicas para el segmento de red inalámbrico que está conectado directamente al switch de core para su posterior salida a internet.

Determinación del riesgo

Para el proceso de determinación de riesgo se utiliza la formula

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Tanto la probabilidad como la magnitud pueden tomar los siguientes valores:

- 1 = Insignificante (Incluido ninguno)
- 2 = Baja
- 3 = Medio
- 4 = Alto

Probabilidad de Amenaza: Para la estimación de este parámetro se utiliza las siguientes consideraciones

- Interés o atracción por parte de individuos externos
- Nivel de vulnerabilidad
- Frecuencia que ocurren los incidentes

Para la estimación de los valores se utiliza la escala descrita en la Tabla 17.

Tabla 17.
Probabilidad de amenaza

Valor	Criterio
1	No Aplica/No es relevante
2	Existen condiciones que hacen muy lejana la posibilidad del ataque
3	Existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo a largo plazo
4	Ataque es inminente, No existen condiciones internas o externa que impidan el desarrollo del ataque

Fuente: realizado por el autor

Según esta valoración se puede organizar los activos dentro del Data-Center en base a las amenazas de la Tabla 16 según su valoración por la probabilidad de ocurrencia en caso de presentarse las condiciones descritas anteriormente. En la tabla 18 se puede encontrar la probabilidad de las amenazas en la infraestructura.

Tabla 18.
Probabilidad según la amenaza

Valor	Amenaza
	Origen Natural
2	Fuego
2	Daños por agua
2	Desastres Naturales
2	Fuego
	Origen Industrial
2	Fuego
2	Daños por agua
2	Desastres industriales
2	Contaminación mecánica
2	Contaminación electromagnética
2	Avería Fisca/Lógica
2	Corte eléctrico
2	Condiciones inadecuadas
2	Fallo servicios comunicación
2	Interrupción servicios
2	Degradación soportes almacenamiento
	Origen Humano (Accidental)
4	Errores de los usuarios
4	Errores del administrador
3	Errores de monitorización
3	Errores de configuración
3	Difusión de software dañino
3	Errores de encaminamiento
3	Errores de secuencia
3	Escapes de información
4	Alteración accidental de la información
3	Destrucción de la información
3	Fugas de información
3	Vulnerabilidades de los programas
4	Errores de mantenimiento/actualización de programas

2	Errores de mantenimiento/actualización de equipos
2	Caída del sistema por agotamiento de recursos
3	Perdida de equipos
	Origen Humano Deliberado
3	Manipulación de la configuración
3	Suplantación de la identidad del usuario
4	Abuso de privilegios de acceso
4	Uso no previsto
3	Difusión de software dañino
3	Re-encaminamiento de mensajes
3	Alteración de secuencia
4	Acceso no autorizado
4	Repudio
4	Modificación deliberada de la información
2	Destrucción de la información
3	Divulgación de información
3	Manipulación de programas
3	Manipulación de los equipos
4	Denegación de servicio
3	Robo
3	Ataque destructivo

Fuente: Elaborada por el autor

Al momento de calcular el riesgo es imperativo generar una matriz de riesgos como se puede observar en la Figura 8.

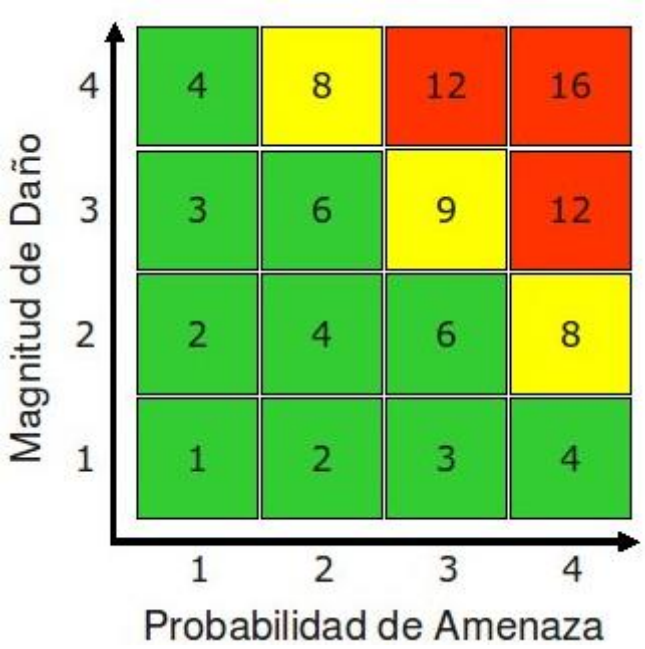


Figura 10. Matriz de Riesgos
Recuperado: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

Donde se puede entender según el color el riesgo que representa quedando de la siguiente manera:

Bajo = 1- 6

Medio = 8 – 9

Alto = 12 - 16

En base la figura 8 se realiza una matriz de riesgos para todas las amenazas y los activos lo que se encuentra referenciado en el Anexo 11. Donde se puede observar los niveles de cada activo según la coloración que indica los niveles de amenaza.

Del Anexo 11 se puede encontrar los resultados con los que se puede calcular el riesgo promedio de todos los valores en base a la probabilidad y magnitud del daño representada en la Tabla 19, que sirve para dar una idea de la condición actual del Data-Center en riesgos.

Tabla 19.
Probabilidad promedio inicial de riesgo del Data-Center

		Probabilidad de Amenaza			
		Origen Natural	Origen Industrial	Origen Humano (Accidental)	Origen Humano (Deliberado)
Magnitud del Daño	Data-Center	5,6	5,6	8,6	9,3

Fuente: Elaborada por el autor

Con la obtención de los resultados en base a cálculos de matriz realizados en Excel y documentados en el Anexo 11 del riesgo que cada activo posee según su amenaza es justificado realizar una implementación de salvaguardas que vienen establecidas en la norma ISO/IEC 27001.

Capitulo IV

Diseño e Implementación del Modelo de Gestión de Seguridad de la Información

En base al análisis de riesgo observado en el capítulo anterior se puede obtener que es importante establecer un modelo de seguridad, para esto se basara el proceso de levantamiento del modelo en la norma ISO 27001 en donde se proveen los objetivos de control necesarios para enfrentar de manera organizada cualquier riesgo que se presente.

Según ISO se sugiere seguir un proceso PDCA (Plan do check act) lo que implica planear, hacer, revisar y actuar.

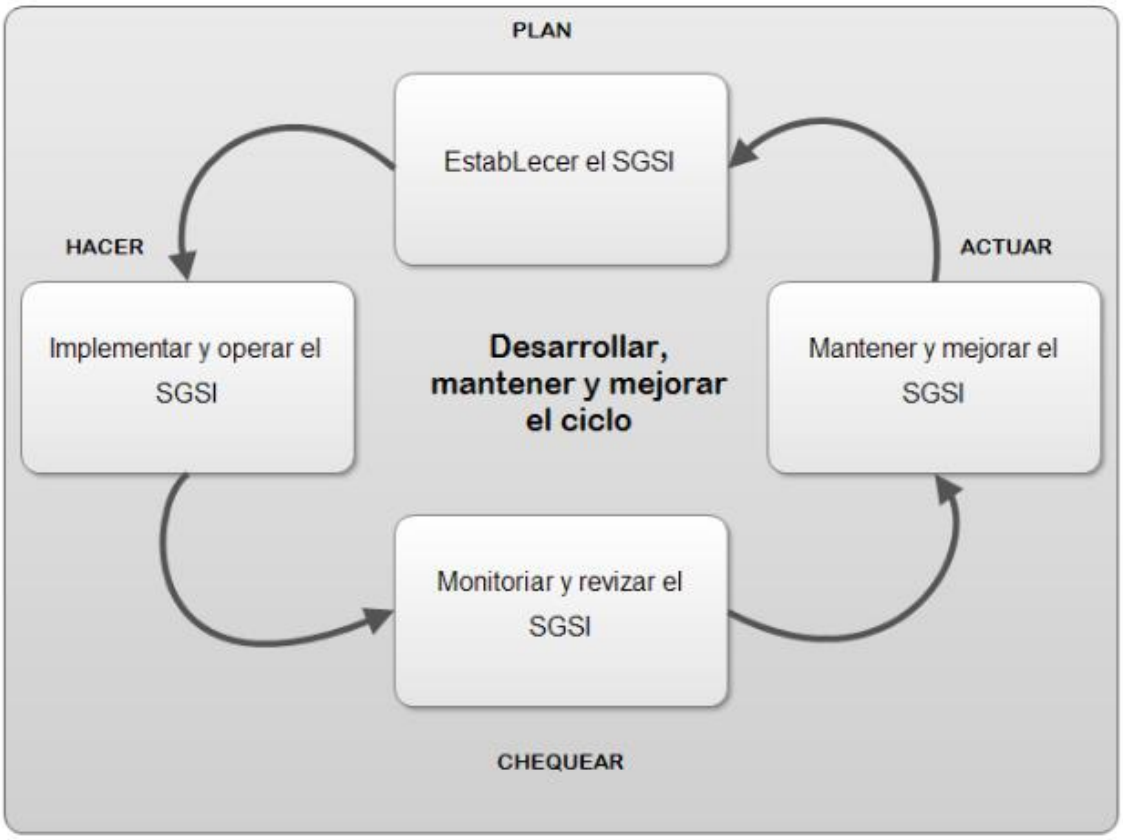


Figura 11. Sistema PDCA
Fuente: realizada por el autor

En la figura 11 se puede observar las fases a realizar en el modelo los cuales son:

- Planear (Establecer el Modelo de gestión de seguridad de la información).

- Hacer (Implementar y operar el modelo de gestión de seguridad de la información)
- Chequear (Monitorizar y revisar el modelo de gestión de seguridad de la información)
- Actuar (Mantener y mejorar el modelo de gestión de seguridad de la información)

4.1.Establecer el Modelo de Gestión de Seguridad de la Información

En este apartado es importante establecer las políticas, objetivos, procesos y procedimientos del modelo de seguridad de la información para manejar el riesgo, mejorar la seguridad del Data-Center y entregar resultados en concordancia con las políticas

4.1.1. Diseño de Políticas y Procedimientos de seguridad de la información

Se procede a la elaboración de las herramientas para el cumplimiento de cada una de las políticas encontradas en la norma ISO/IEC 27001 hay que destacar que dentro de cada una se cuenta con un objetivo de control y controles los cuales indican que acciones se pueden tomar y pueden presentar soluciones tanto manuales, administrativas, procedimentales y por aplicación de software para la implementación de un modelo de gestión de seguridad de la información.

Se plantea un modelo que servirá para mejorar las condiciones iniciales del Data-Center las cuales se presentaron en la Tabla 19.

Diseño de objetivos de control según la norma ISO/IEC 27001

Para la elaboración de políticas se sigue los lineamientos de la norma ISO/IEC 27001 en donde nos indica el establecimiento del modelo de gestión de seguridad de la información, dentro de este apartado se procede a identificar los objetivos de control tomados en cuenta para la realización del manual de procedimientos y las herramientas implementadas para el

cumplimiento de cada una, los objetivos de control se los selecciono de la norma ISO/IEC 27001 en base a los riesgos que necesitan ser abordados inmediatamente los cuales son amenazas de origen humano tanto accidental como deliberado enfocados a la seguridad lógica del Data-Center.

Los objetivos de control seleccionados son:

1. Política de Seguridad de la Información
2. Organización de seguridad de la información
3. Gestión de los Activos
4. Gestión de Comunicaciones y Operaciones
5. Control de Acceso
6. Gestión de incidentes en la seguridad de la información
7. Cumplimiento

El manual de políticas de seguridad para el Data-Center se elaboraron en base a la norma ISO/IEC 27002, tomando en cuenta los objetivos de control mencionados para de esta manera darle una presentación formal a todos los objetivos de control que se tomara en cuenta para el establecimiento del modelo de seguridad de la información.

Políticas de seguridad de la información

Dentro del primer parámetro políticas de seguridad de la información se tomará en cuenta los objetivos y controles los cuales están determinados en la normativa ISO/IEC 27001 los cuales se desglosarán en la Tabla 20 y se adaptaron al documento global de políticas que se encuentra referenciado en el Anexo 12.

Tabla 20.
Objetivo de control Política de seguridad de la información

Política de seguridad de la información	
Objetivo de control	**Control**
Documentar la política de seguridad de información	La administración debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

Fuente: Elaborada por el autor

Para el cumplimiento de este objetivo de control se procede a la elaboración del documento de las políticas de seguridad de la información que se encuentra en el Anexo 12 y se procederá a la entrega a los encargados del Data-Center para su revisión y aprobación.

Organización de seguridad de la información

Dentro de este parámetro presentado en la normativa se encuentran definidos los objetivos de control y controles presentados en la Tabla 21, se tomaron en cuenta los objetivos aplicables a la organización, en el momento que se evolucione la prestación de servicios y usuarios finales se procederá a implementar los objetivos descartados.

Tabla 21.
Objetivo de control Organización de Seguridad de la Información

Organización de Seguridad de la información	
Objetivo de control	**Control**
Compromiso de la administración con la seguridad de la información	La administración debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la información.
Coordinación de la seguridad de la información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
Proceso de autorización para los medios de procesamiento de información	Se deben definir e implementar un proceso de autorización administrativa para los nuevos medios de procesamiento de información.

Contacto con autoridades	Se debe mantener los contactos apropiados con las autoridades.
Contacto con grupos de interés	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
Revisión independiente de la seguridad de la información	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

Fuente: Elaborada por el autor

Compromiso de la administración con la seguridad de la información: Al momento de entregar el manual de políticas se acepta el compromiso de realizar cualquier actividad que contemple la seguridad de la información

Coordinación de la seguridad de la información: Cada actividad será organizada y elaborada conforme al diagrama de procedimiento descrito en la Figura12.

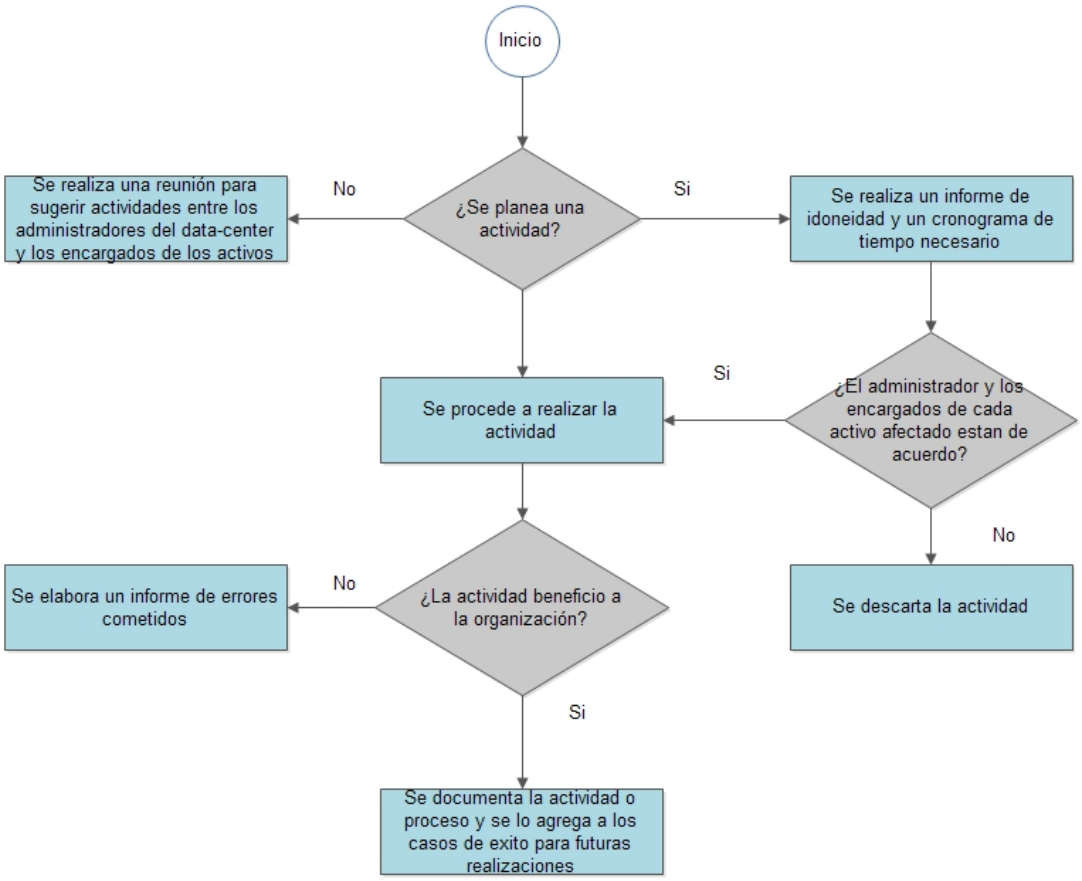


Figura 12. Proceso de coordinación de seguridad de la información
Fuente: realizada por el autor

Asignación de responsabilidades de la seguridad de la información: La asignación de responsabilidades es competencia de el o los administradores de red los cuales se encargarán de asignar los responsables de el o los activos que se encuentran en el Data-Center, en la actualidad los responsables de cada activo se encuentran definidos en la Tabla 3

Proceso de autorización para los medios de procesamiento de información: Para la autorización de procesos se realizará un procedimiento establecido en la Figura 11.

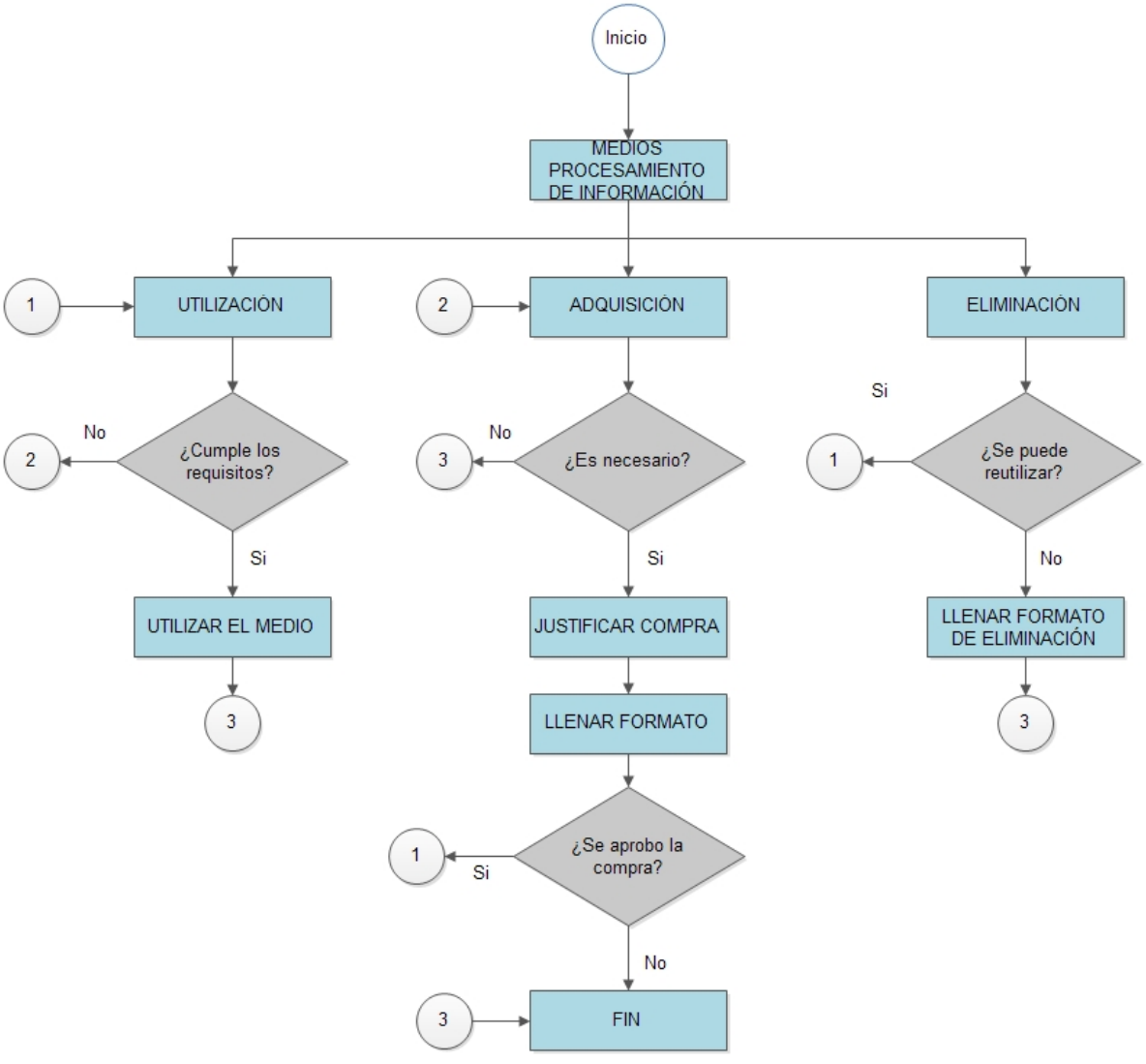


Figura 13. Procedimiento de medios de procesamiento de información.
Fuente: realizada por el autor

Contacto con autoridades: Cada suceso o incidente será informado a las autoridades por medio de un formato predeterminado de reporte de incidencias que se encuentra referenciados en el Anexo 13.

Contacto con grupos de interés: Como administradores de red o personas encargadas de los servicios y servidores es imperativo la realización de convenios con asociaciones especializadas en seguridad, cada acuerdo debe ser formalizado renovado en calidad de beneficio mutuo.

Revisión independiente de la seguridad de la información: El proceso de evaluación independiente puede ser realizado por los grupos con los que se tiene acuerdos o compromisos y se realizara previa autorización y planificación de las personas que conforman el departamento encargado del Data-Center.

Gestión de los Activos

Como organización lo más importante es la identificación de los activos para lo cual se establecen unas políticas basadas en la norma ISO/IEC 27001 donde se especifican los controles y objetivos de control los cuales se referencian en la Tabla 22.

Tabla 22.
Gestión de Activos del Data-Center

Gestión de Activos	
Objetivo de control	**Control**
Inventario de Activos	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de activos importantes.
Propiedad de los activos	Toda la información y los activos asociados con los medios de procesamiento de la información deben ser propiedad de una parte designada de la organización.
Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable con los medios de procesamiento de la información.
Lineamientos de clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
Etiquetado y manejo de información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la

	información en concordancia con el esquema de clasificación adoptado por la organización.

Fuente: Elaborada por el autor

Para el cumplimiento de los controles especificados se procede a realizar una política que se encuentre referenciada en el Anexo 12, además de un inventario de los activos mediante fichas técnicas las cuales cuentan con una propuesta de elaboración y se encuentran referenciadas en el Anexo 2.

Gestión de las comunicaciones y operaciones

Hay que tener asegurados la operación correcta y segura de los medios de procesamiento de la información dentro de este apartado es necesario identificar los objetivos y controles establecidos por la normativa los cuales están descritos en la Tabla 23.

Tabla 23.
Gestión de Comunicaciones y Operaciones

Gestión de comunicaciones y operaciones	
Objetivo de control	**Control**
Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación; y se deben poner a disposición de todos los usuarios que los necesiten.
Gestión del cambio	Se deben controlar los cambios en los medios y sistemas de procedimiento de la información.
Segregación de deberes	Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización
Separación de los medios de desarrollo y operacionales	Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de información
Gestión de capacidad	Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido
Aceptación del sistema	Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones versiones nuevas y se deben llevar a cabo pruebas adecuadas.
Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de los ataques maliciosos y se deben aplicar procedimientos de conciencia apropiados.

Back-up	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente.
Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad y aplicaciones utilizando la red, incluyendo la información de tránsito.
Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente
Gestión de los medios removibles	Deben existir procedimientos para la gestión de medios removibles
Eliminación de medios	Los medios deben ser eliminados usando procedimientos formales y de una manera segura cuando ya no se les requiere.
Seguridad de la documentación del sistema	Se debe proteger la documentación de un acceso no autorizado

Fuente: Elaborada por el autor

Para el cumplimiento de los siguientes objetivos de control:

- Procedimientos de operación documentados
- Gestión del cambio
- Segregación de deberes
- Separación de los medios de desarrollo y operacionales
- Aceptación del sistema

Se elaboro un formato de procedimientos que se encuentra en el Anexo 14 en donde se considera los controles establecidos en los objetivos para de esta manera documentar las actividades realizadas, a su vez se elaboró un procedimiento que se describe en la Figura 14.

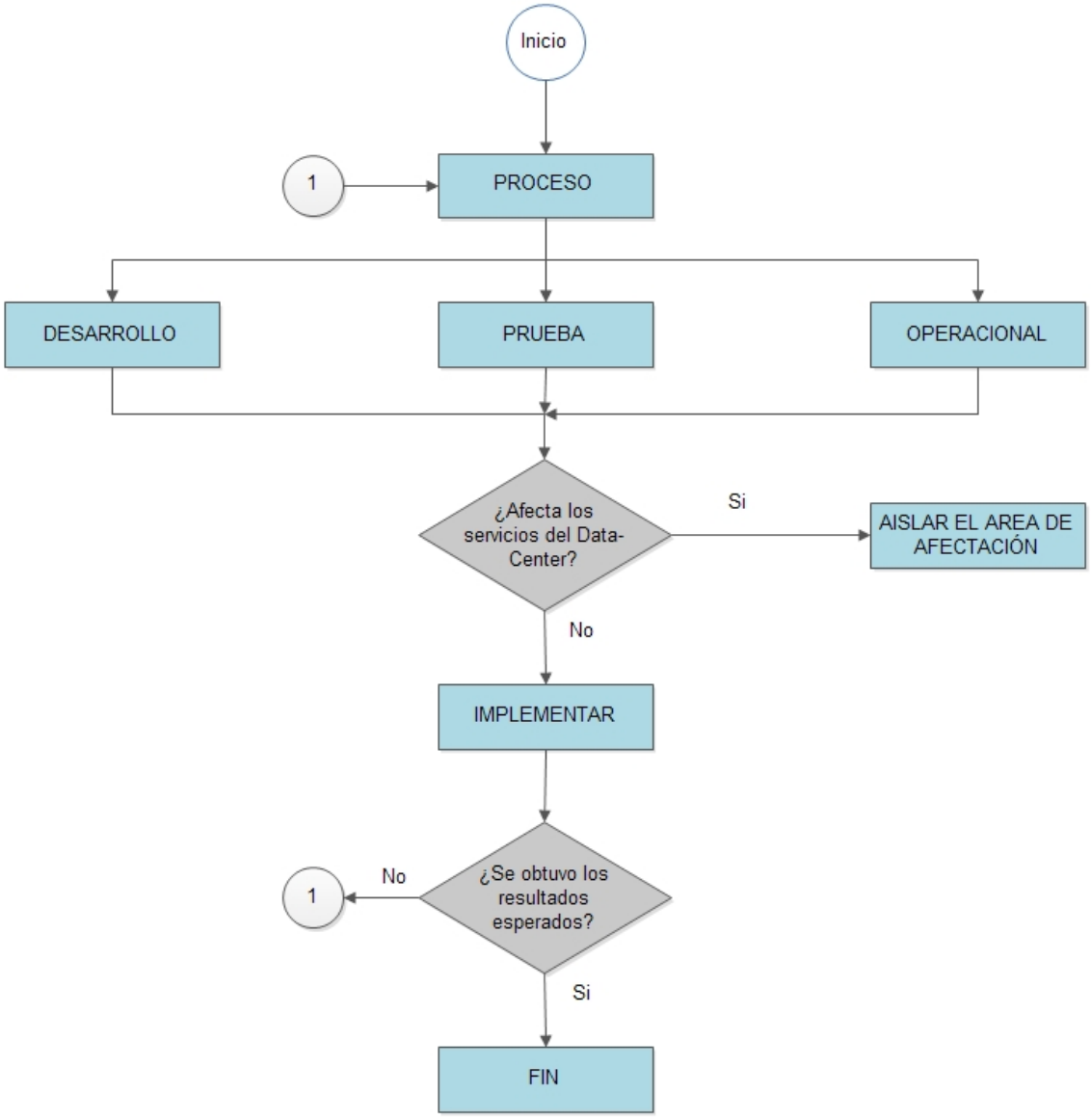


Figura 14. Procedimiento para la realización de un proceso
Fuente: realizada por el autor

Se implementará un software que permita cumplir con los siguientes objetivos de control:

- Gestión de capacidad
- Back-up
- Controles de red
- Seguridad de los servicios de red

Cada uno de los que será tomado en cuenta para la selección de software asegurando que entre dentro de sus características funcionales.

Para el siguiente grupo de objetivos de control que están descritos a continuación:

- Gestión de los medios removibles
- Eliminación de medios
- Seguridad de la documentación del sistema

En la figura 15 se procede a identificar los procesos que se realizaran y los formatos que se solicitan se encuentran en el Anexo 15 y Anexo 16, además es importante destacar que para el objetivo central se generó una política referenciada en el Anexo 12.

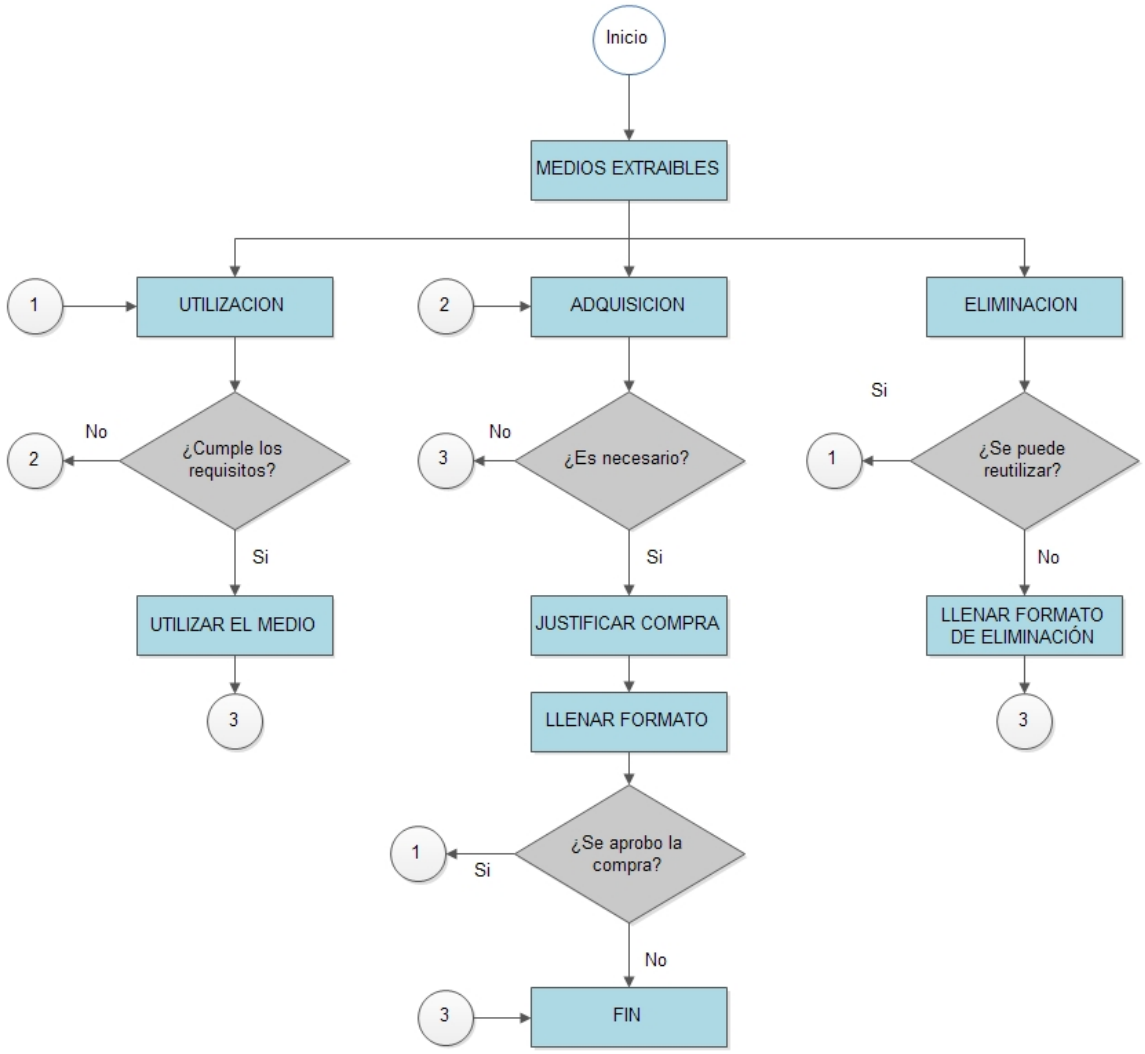


Figura 15. Procedimiento de medios extraíbles
Fuente: realizada por el autor

Control de Acceso

En la Tabla 24 se identifican los objetivos de control especificados en la normativa para este apartado, los cuales se deberán revisar y cumplir con los controles necesarios para el diseño del modelo de gestión de seguridad de la información.

Tabla 24.
Gestión de Comunicaciones y Operaciones

Control de acceso	
Objetivo de control	**Control**
Gestión de privilegios	Se debe restringir y controlar la asignación y uso de los privilegios
Gestión de la clave del usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal.
Revisión de los derechos de acceso del usuario	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos reguladores utilizando un proceso formal.
Uso de clave	Se debe requerir que los usuarios sigan buenas prácticas de seguridad de la selección y uso de claves.
Política sobre el uso de servicios en red	Los usuarios solo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
Autenticación del usuario para conexiones externas	Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
Identificación del equipo en red	Se debe considerar la autenticación automática del equipo como medio para autenticar las conexiones desde equipos y ubicaciones específicas.
Protección del puerto de diagnóstico remoto	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
Segregación en redes	Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
Control de conexión	Se deben restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los limites organizacionales, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales.
Control de ‘routing’ de redes	Se deben implementar controles routing para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales
Procedimiento de registro en el terminal	Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro
Identificación y autenticación del usuario	Todos los usuarios deben tener un identificador singular para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario

Sistema de gestión de claves	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de claves
Limitación de tiempo de conexión	Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo
Restricción al acceso a la información	Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida
Aislamiento del sistema sensible	Los sistemas sensibles deben tener un ambiente de computo dedicado

Fuente: Elaborada por el autor

Para cumplir con los objetivos de control especificados se realiza una identificación de los controles requeridos donde se alineará los objetivos de control que pueden resolverse en conjunto.

Gestión de privilegios: Este objetivo de control es el responsable de asignar a un usuario el tipo de privilegio que tiene dentro de un determinado servidor, dentro de lo que es privilegio en manejo de ficheros e información se encuentran los de lectura y escritura, el primero permite que un usuario pueda revisar los archivos que contiene el servidor pero no permite su modificación o eliminación, el segundo permite un acceso total al sistema por lo cual el administrador de la red o el encargado del servidor debe autorizar el acceso por el riesgo que conlleva. Dentro del Data-Center actualmente solo los administradores de red y el encargado tienen el acceso físico o lógico a los equipos por lo cual solo se procede a generar una política que se encuentra referenciada en el Anexo 12.

Gestión de clave de usuario y revisión de los derechos de acceso del usuario: Dentro de cada uno de los servidores implementados actualmente se encuentran bases de datos propias para el manejo de claves, en los servidores más importantes solo existe un acceso de root que lo maneja el encargado del servidor y lo conoce a su vez el administrador de red.

Uso de claves: Para la utilización de claves de cada usuario y administrador se genera una política que esta descrita en el Anexo 12.

Control de routing de redes: En base al levantamiento de información documentado en el capítulo III, en base a esto se puede definir una nueva propuesta de arquitectura de red que permita separar los servidores del resto de la infraestructura como se puede observar en la Figura 16.

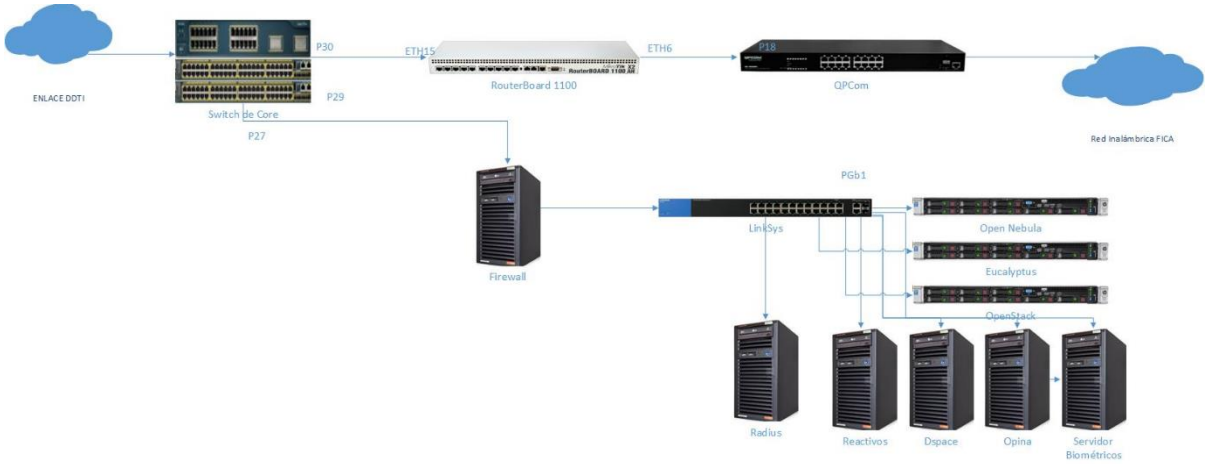


Figura 16. Procedimiento de medios extraíbles
Fuente: realizada por el autor

Identificación y autenticación del usuario: Existe un sistema implementado en cada uno de los servidores que interactúan con el usuario final para su identificación, dentro de los cuales se puede destacar los sistemas que actualmente manejan autenticación e identificación del usuario:

- Opina: Este sistema cuenta con su propia base de datos y su identificación de usuarios, la encriptación que utiliza es md5, además el administrador puede mantener un registro de accesos y privilegios en base al diagrama general manejado en la Figura 16.
- Mikrotik y Servidor Radius: Estos equipos se encargan de la gestión de usuarios con acceso a internet manejados de manera independiente por el encargado del sistema y permite asignar un direccionamiento, un acceso, un control de ancho de banda y un identificador para cada usuario final de la red inalámbrica de la facultad.

Los demás servidores manejan un sistema independiente gestionado por el encargado del activo el cual tiene acceso root y cualquier tipo de acceso como invitado está restringido.

El resto de objetivos de control que se encuentran en la Tabla 24 son los siguientes:

- Autenticación del usuario para conexiones externas
- Identificación del equipo en red
- Protección del puerto de diagnóstico remoto
- Segregación en redes
- Control de conexión
- Limitación de tiempo de conexión
- Restricción al acceso a la información
- Aislamiento del sistema sensible

Para cumplir con todos los controles de cada objetivo de control se propone la implementación de un software firewall que estará ubicado como se puede observar en la Figura 16, es importante destacar que el sistema seleccionado debe cumplir con lo antes expuesto.

Gestión de incidentes en la seguridad de la información

En base al modelo encontrado en el Data-Center se puede seleccionar los siguientes objetivos de control, los cuales se centran en la gestión de la seguridad de la información.

El proceso de gestión viene de la mano con la seguridad informática porque permite llevar un control de los incidentes que se ocasionan la parte lógica de la red y que ocasionan fallos que afectan las funcionalidades de los servidores y servicios alojados en el Data-Center.

Tabla 25.
Gestión de incidentes en la seguridad de la información

Gestión de incidentes en la seguridad de la información	
Objetivo de control	**Control**
Reporte de eventos en la seguridad de la información	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados.
Reporte de debilidades en la seguridad	Se deben requerir que todos los empleados contratistas y terceros usuarios de los sistemas y servicios de la información tomen nota y reporten cualquier debilidad observada o sospechosa en la seguridad de los sistemas o servicios.
Responsabilidad y procedimientos	Se deben establecer las responsabilidades y procedimientos generales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de información.
Aprendizaje de los incidentes en la seguridad de la información	Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información
Recolección de evidencia	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad e la información involucra una acción legal (sea civil o criminal), se de recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.

Fuente: Elaborada por el autor

Para el cumplimiento de los objetivos de control expuestos en la Tabla 25 es importante destacar que se utilizara un software firewall que tenga las características funcionales necesarias.

Cumplimiento

Hay que destacar que como parte de los controles toda la normativa contempla una normativa con los parámetros y responsabilidades de los administradores de red y encargados de los servicios o activos que integran el Data-Center la política. Cada uno no de los controles ha sido descrito en su totalidad y el plan de contingencia se realizará con sugerencias de sistemas que se pueden implementar para mejorar la funcionalidad de las políticas y la normativa.

4.2.Firewall

La implementación del firewall se plantea como una solución tanto a la arquitectura de red como a los objetivos de control de la normativa que se mencionaron serian solucionados por medio de un software, para la elaboración de este rediseño se plantea el aislamiento de los servidores por medio de un equipo de características mínimas per funcionales que permitan generar un DMZ entre el switch de core y los servidores tanto físicos como virtualizado que se encontraban en la infraestructura.

Como se puede observar en la figura 16, la propuesta de arquitectura de red elimina un switch y se mantiene el switch linksys que posee 2 puertos gigabit Ethernet y 22 puertos fast Ethernet para manejar los 6 servidores activos que se encuentran actualmente en funcionamiento. En la figura 17 se puede observar de manera aislada como se encontrará ubicado el firewall y los servidores una vez realizada su implementación.

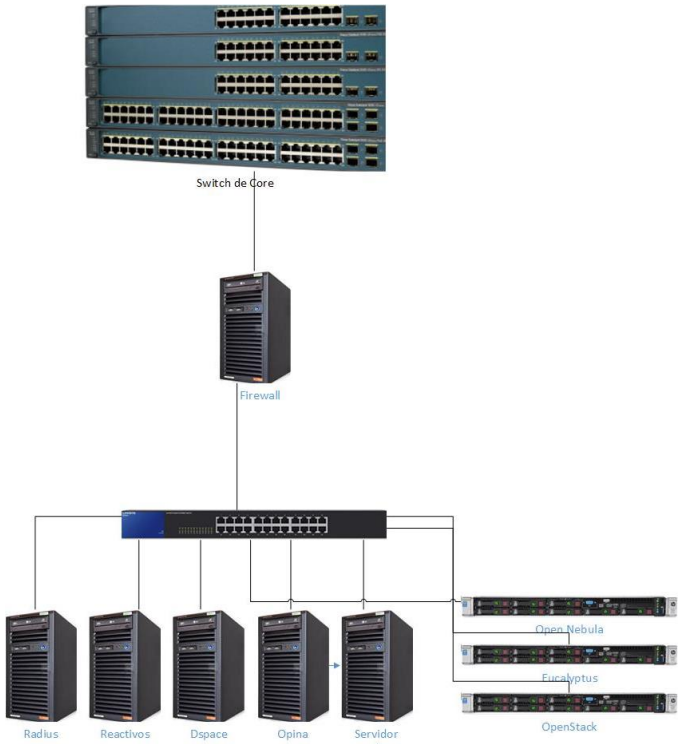


Figura 17. Procedimiento de medios extraíbles
Fuente: realizada por el autor

Para el cumplimiento de estos objetivos de control y selección de software se realizó una investigación de 2 software que se pueden implementar en un servidor físico con las características que se asignó al proyecto, estos sistemas se describen a continuación.

4.2.1. ClearOs

Es una plataforma de software de código abierto que simplifica la utilización en redes considerándose una de los sistemas híbridos de bajo costo para mejorar las TICs de empresas PYMES. El valor de esta herramienta consiste en la integración de tecnologías de código abierto haciendo fácil de utilizar.

Las características que se pueden destacar son:

- Firewall IPtables.
- Escaneo de virus y spam a través de la pasarela de paso para tráfico http
- Sistema de detección de intrusos SNORT
- Red Privada Virtual (PPPT,IPSec,OpenVpn)
- Proxy con filtrado de contenidos (Squid, DansGuardian)
- Servicios e-mail (Webmail, Postfix, SMTP, POP3/s, IMAP/s)
- Groupware (Kolab)
- Base de Datos y Web Server (LAMP)
- Servidor de archivos y servicios de impresión (Samba and CUPS)
- Flexshares (almacenamiento unificado multiprotocolo que emplea CIFS, HTTP/S, FTP/S, and SMTP)
- MultiWAN (Diseño Internet tolerante a fallos)
- Informes de estadísticas de Sistema y servicios (MRTG y otros)

4.2.2. Endian Firewall

Es una distribución de código abierto basada en Linux, que no solo se especializa en cortafuegos, además es una solución integral para proteger una red de amenazas externar, ofreciendo todos los servicios que brinda un UTM, además es fácil de utilizar e instalar.

Sus características a destacar son las siguientes:

- Establecimiento de reglas de firewall de entrada y salida
- Nat (traducción de direcciones de red)
- Soporte para dns dinámicos
- Soporte para dmz
- Interfaz de administración web mediante protocolo https
- Gráficos detallados de las interfaces de red
- Detalle de todas las conexiones activas
- Log detallado de todos los procesos del sistema
- Servidor dhcp
- Permite implementar comunicaciones seguras con otras sedes o clientes remotos a través de vpn
- Antivirus y filtrado de contenido para un acceso a internet más seguro
- Manejo de proxy
- Enrutamiento
- Antivirus y anti spam para el correo electrónico
- Alta disponibilidad
- Manejo de redes inalámbricas seguras

Interfaz de usuario

En la Tabla 26 se puede observar si los sistemas seleccionados poseen un acceso tanto de interfaz web como SSH para la configuración del sistema por parte del administrador de la red.

Tabla 26. Interfaz administrador comparación
Interfaz administrador comparación.

Software	Interfaz Web	SSH
ClearOs	Si	Si
Endian Firewall	Si	Si

Fuente: realizado por el autor

Hardware

Para la selección de la plataforma a implementar es importante tener una optimización de las características del equipo asignado para el proyecto y por eso de cada una de las páginas de los sistemas seleccionados se puede destacar las características mínimas para su funcionamiento especificadas en la Tabla 27.

Tabla 27. Características mínimas de hardware
Características mínimas de hardware

Características	**ClearOS**	**Endian Software**
Procesador/CPU	5 usuarios 500MHz 10 usuarios 1GHz 50 usuarios 2GHz 200 usuarios 3GHz	Pentium III 1GHz
Memoria/RAM	5 usuarios 512GB 10 usuarios 1GB 50 usuarios 1.5GB 200 usuarios 2GB	512MB hasta 1GB
Disco Duro	1GB para instalación y logs, más memoria es opcional	Recomendado 8GB

Fuente: realizado por el autor

Actualizaciones y Soporte

La plataforma que se seleccione tiene que contar con actualizaciones constantes debido a que los atacantes informáticos y las amenazas están en constante evolución, en tal virtud es necesario saber el periodo que se actualiza el software y sus herramientas además de si un centro de soporte en caso de necesitar ayuda por posibles fallos o errores en su configuración, en la Tabla 28 se encuentran descritos los periodos de actualización de la base de datos de cada herramienta.

Tabla 28.
Características Firewall

Características	ClearOS	Endian Firewall
Actualizaciones	Mensual	Mensual
Soporte	Si	Si

Fuente: realizado por el autor

4.2.3. Selección Del Software Firewall Mediante La Norma ISO/IEC/IEEE 29148:2011

En el apartado anterior se describió una breve determinación de características, pero para la implementación de un software que permita cumplir con los objetivos de control de la norma ISO/IEC 27001 es importante realizar una comparación por medio de características funcionales y no funcionales de un software y de esta manera seleccionar la mejor opción.

Propósito:

En base a la norma ISO/IEC 27001 es necesario seleccionar un software que permite cumplir con los objetivos de control mencionados en el apartado anterior y que se definieron como posibles soluciones mediante una implementación de un software.

Alcance:

- Proteger la información en servidores y servicios.
- Segregar las redes en función de sus servicios y puertos de comunicación.

- Seguridad de las comunicaciones en servidores accesibles por redes públicas.
- Protección de las transacciones que requieran acceso al Data-Center.
- Protección ante malware y ataques informáticos.

Perspectivas del Producto

Se requiere que la plataforma seleccionada permita una integración de sus herramientas a la red de forma amigable con el usuario final que permita separar los servicios y generar una DMZ para proteger la información, a su vez que se cumplan los objetivos de control presentados por la norma ISO/IEC 27001.

Funciones del Producto

El presente proyecto al encontrarse integrado en la Facultad de Ingeniería y Ciencias Aplicadas es necesario que cumpla las siguientes funcionalidades:

- Resguardar la información contenida en los servidores alojados en el centro de datos.
- Proteger de los ataques informáticos que provengan de la intranet e internet
- Generar un sistema transparente para el usuario final y que brinde las seguridades necesarias ante posibles eventos
- Recopilar los ataques realizados al centro de datos mediante logs y alertas en su interfaz web
- El administrador del centro de datos será el encargado de revisar los informes de alerta y tomar las acciones adecuadas para gestionar las reglas de acceso.

Características del usuario

Este software debe mantenerse transparente para el usuario final, pero a su vez presentar las herramientas necesarias para alcanzar la mejora de los niveles de confidencialidad, integridad y disponibilidad de la información.

Limitaciones

Las limitaciones que puede encontrar el software firewall seleccionado pueden ser las siguientes:

- Capacidad de los equipos enrutadores.
- Capacidad del equipo manejado por el usuario final.
- Errores lógicos debido a fallos en la configuración en los servidores.
- Errores físicos por parte de la infraestructura del Data-Center.

Suposiciones y Dependencias

Se tendrá en cuenta las siguientes suposiciones:

- El equipo donde se procederá a la instalación del software cumplirá con todos los requisitos mínimos de hardware.
- Cada uno de los usuarios finales es un posible atacante.
- La información transmitida entre servidor y usuario final es prioridad máxima que requiere resguardo constante para evitar posibles alteraciones.
- Todos los servidores están expuestos a ataques informáticos en cualquier momento.
- El administrador de red estará constantemente verificando mediante un interfaz web por posibles alertas en la seguridad.

Requisitos Específicos

En este apartado se procede a detallar las características necesarias para la implementación de un firewall que nos permita cumplir con la mayor cantidad de políticas de seguridad.

- Gestión de incidentes en la seguridad de la información
- Gestión de comunicaciones y operaciones
- Control de acceso

Requisitos comunes de las interfaces

Es necesario identificar los requisitos comunes que se requiere en las interfaces, en este apartado se destaca que es necesario contar en el equipo dos NIC con capacidad gigabit Ethernet.

Interfaces de usuario

Al ser un entorno orientado a la seguridad de la red el interfaz de usuario solo será habilitado para el administrador de la red y personas que previamente soliciten acceso, ya que la información que maneja es de muy alta importancia porque permite conocer el tipo se información que manejan los servidores.

Interfaces de Hardware

Es necesario basar las características en las especificaciones de los dos sistemas para funcionar de manera óptima, en la Tabla 27 se observa que lo minino para desempeñar un funcionamiento óptimo es un procesador de 1GHz, 1Gb en memoria RAM y 10 Gb de Disco duro para el almacenamiento de ficheros de reportes, procesamiento de datos enrutados y logs generados por el sistema.

Interfaces de software

El interfaz que manejara la plataforma seleccionada debe ser amigable con el administrador de la red además de brindar todas las facilidades para el control de reportes, estados del firewall y la información que pasa a través de el en todo momento, asegurando que las reglas de acceso establecidas se estén cumpliendo.

Restricción de memoria

No existen restricciones de memoria en el software, pero es importante dimensionar las características para no desperdiciar los recursos del equipo que se asignó para el proyecto.

Requisitos funcionales

En la Tabla 29 se resumen los requisitos funcionales necesarios en base a los objetivos de control a cumplir, y se utilizara una escala del 1 a 3 para identificar la priorización de cada herramienta según el software de la siguiente forma:

3 Alta, 2 Media, 1 Baja

Tabla 29.
Requisitos y características

Requisito	**Características**	**Prioridad**	
		ClearOS	Endian Firewall
Gestión de incidentes en la seguridad de la información	Reporte de eventos en la seguridad de la información	2	3
	Reporte de debilidades en la seguridad	2	3
	Recolección de evidencia	3	3
	Reporte de eventos en la seguridad de la información	1	3
Gestión de comunicaciones y operaciones	Gestión de capacidad	2	3
	Control contra software malicioso	3	3
	Controles de red	3	3
	Seguridad de los servicios de red	3	3
Control de acceso	Aprendizaje de los incidentes en la seguridad de la información	1	3
	Autenticación del usuario para conexiones externas	1	1
	Identificación del equipo en red	1	2
	Protección del puerto de diagnóstico remoto	3	3
	Segregación en redes	1	3

	Control de conexión	3	2
	Limitación de tiempo de conexión	2	3
	Restricción al acceso a la información	3	3
	Aislamiento del sistema sensible	3	3
TOTAL		37	47

Fuente: realizado por el autor

Requisitos no funcionales

Dentro de la Tabla 30 se encuentran los requisitos que el software tiene incluidos pero que no son indispensables para el cumplimiento de los objetivos de control, y algunas características extra que vienen integradas en firewall.

Tabla 30.
Requisitos y descripción

Requisito	**Descripción**	**Prioridad**	
		ClearOS	Endian Firewall
Gestión del ancho de banda	Asignar ancho de banda basado en Usuarios	3	2
	Asignar ancho de banda basado en Aplicaciones	2	2
	Asignación de ancho de banda basada en reglas para el tráfico web	2	2
Administración de red	Configuración de red rápida y sencilla	1	3
	Servidor DHCP	2	3
	Servicio de DNS directo compatible con almacenamiento en caché	3	3
	Soporte para múltiples LAN dentro de la misma red	2	3
Conectividad Remota	OpenVPN Server con una interfaz web rápida y sencilla para la gestión de clientes VPN	1	2
	Soporte de cliente VPN de sitio a sitio	1	2
	TOTAL	17	20

Fuente: realizado por el autor

Requisitos de Rendimiento

Según el sistema implementado en el Data-Center es necesario proteger los servicios y servidores implementados en los dos switch de distribución que están descritos en la situación actual, al referirse a una protección de las DMZ es necesario escoger una plataforma con las mejores características.

Justificación

En base al comparativo realizado por medio de la Tabla 29 y Tabla 30 se puede concluir que Endian Firewall tiene mayor prioridad en los objetivos de control requeridos según ISO/IEC 27001.

La plataforma Endian firewall posee varias distribuciones, entre ellas se tiene community que cuenta con la mayoría de sus herramientas gratuitas y las siguientes versiones que implementan ciertas ventajas como soporte continuo para las versiones de pago.

4.2.4. Implementación de Endian Firewall

La topología que se presenta en la Figura 13, es la que se implementara en el Data-Center con el software Endian, que cumple con todos los objetivos de control de manera eficiente, para el procedimiento de instalación se utilizara el equipo designado y se realizara el procedimiento referenciado en el Anexo 18.

Para la implementación del software y el direccionamiento es importante destacar el direccionamiento actual de la topología lógica la cual se puede observar en la tabla 31, hay que denotar que se presentara un direccionamiento propio para generar la DMZ de cada uno de los servidores alojados, la propuesta de direccionamiento se encuentra determinada en la Tabla 31.

Tabla 31.
Direccionamiento servidores Data-Center

RED	Subred	IP	Gateway
INTERNA DATA-CENTER	10.24.8.0/24		10.14.8.1
OPINA	10.24.8.0/24	10.24.8.X	10.14.8.1
VOZ/IP	10.24.8.0/24	10.24.8.X	10.24.8.1
REACTIVOS	10.24.8.0/24	10.24.8.X	10.24.8.1

Fuente: realizado por el autor

Se implementará la arquitectura lógica presentada en la Figura 18 y se utilizará el direccionamiento presentado en la Tabla 32.

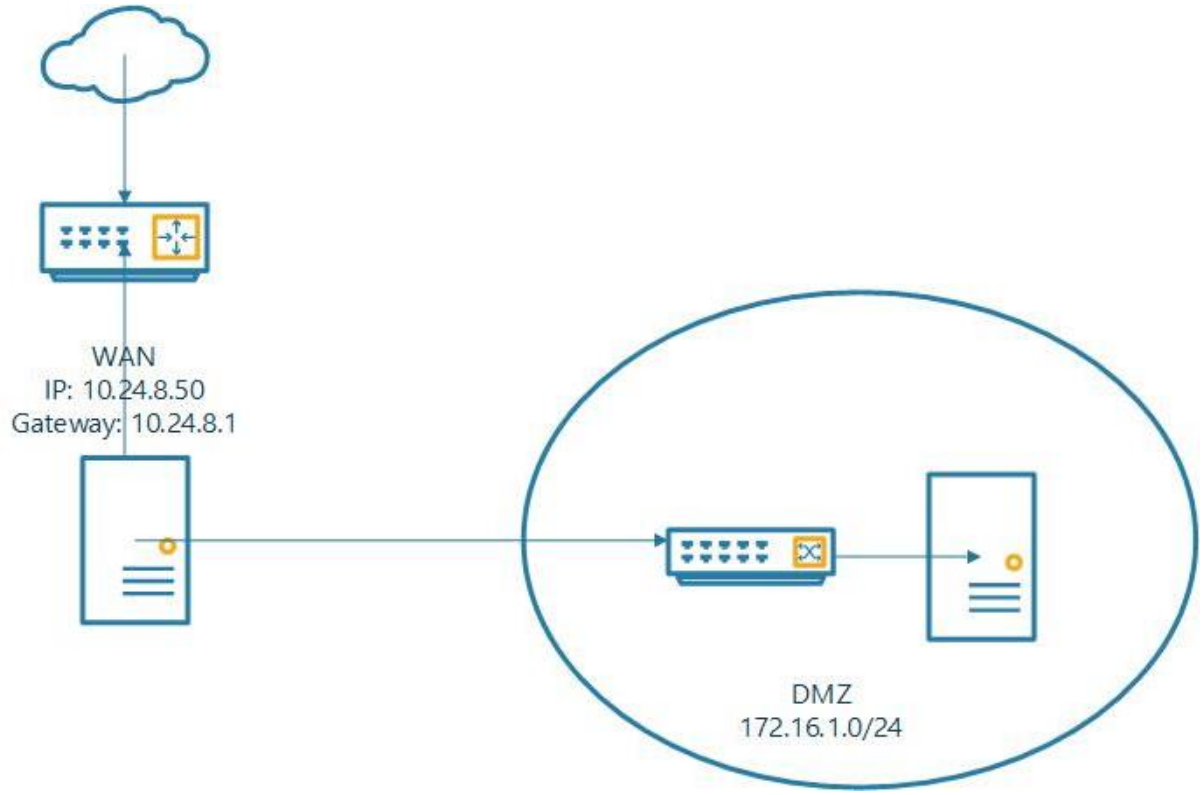


Figura 18. Topología Lógica con DMZ
Fuente: realizado por el autor

Tabla 32.
Direccionamiento servidores Data-Center

RED	Subred	IP	Gateway
IP ENDIAN	10.24.8.0/24	10.24.8.50	10.14.8.1
DMZ	172.16.2.0/24	172.16.2.1	172.16.2.1
OPINA	172.16.2.0/24	172.16.2.15	172.16.2.1
VOZ/IP	172.16.2.3/24	172.16.2.3	172.16.2.1
REACTIVOS	172.16.2.7/24	172.16.2.7	172.16.2.1

Fuente: realizado por el autor

Para la configuración del software hay que acceder por medio del interfaz web por medio de la dirección ip asignada al interfaz Verde o LAN temporal que se utilizara para configuración de las interfaces, la dirección asignada es https://172.16.1.1:10443, en la primera ocasión de acceso se requiere un usuario y contraseña que por defecto son admin y endian respectivamente.

Una vez dentro del sistema como se puede observar en la Figura 19 se solicita que se cambie las contraseñas de root para el acceso ssh y la de admin para el acceso al interfaz web.

Figura 19. Cambo de contraseña Endian Firewall
Fuente: Realizado por el autor

Luego de aceptar el cambio de contraseña se reiniciará el navegador, pidiendo las nuevas credenciales de acceso, y presenta la configuración de los interfaces de red donde se asignará el direccionamiento según la Tabla 32, dentro de Endian existen cuatro tipos de redes que se pueden configurar por defecto:

- Naranja.- Se utiliza para designar la porción de red para los servidores accesibles desde la internet o DMZ.
- Azul.- Utilizada para los usuarios de la red inalámbrica
- Verde.- Para los usuarios de la red LAN
- Roja.- Esta designación es para el enlace WAN.

Dentro de la configuración se procede a asignar el direccionamiento de la red naranja o DMZ cono se observa en la Figura 20.

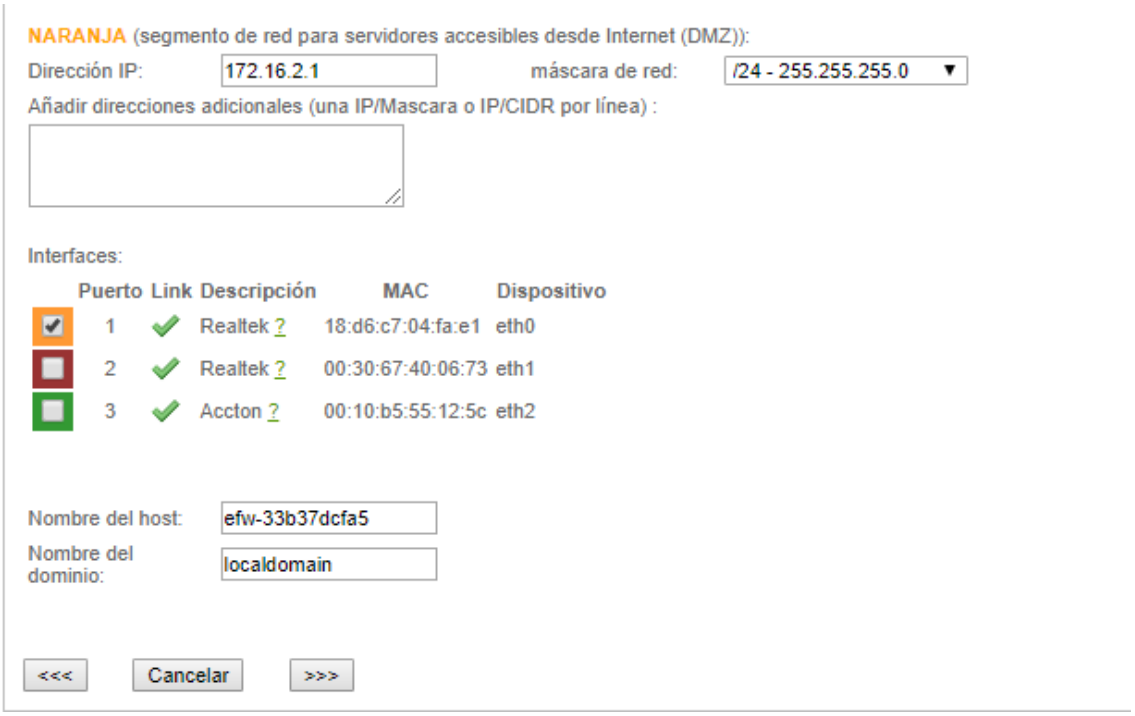


Figura 20. Asignación direccionamiento DMZ
Fuente: Realizado por el autor

Previo esto es necesario la configuración de la red roja o WAN con el direccionamiento asignado previamente como se observa en la figura 21, hay que destacar que el mismo software permite ocultar la dirección MAC de la NIC que se enlaza a la internet.

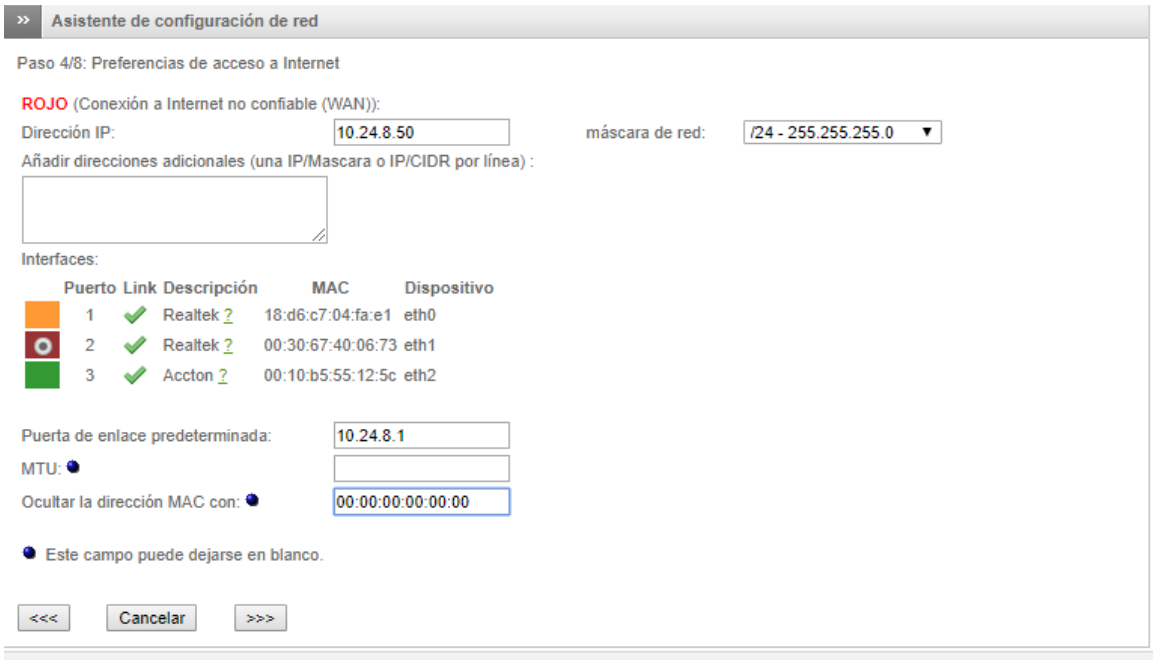


Figura 21. Asignación direccionamiento WAN
Fuente: Realizada por el autor

Una vez confirmada la configuración cabe aclarar que al asignar la DMZ en la red naranja se asigna una política de Denegar Todo que asegura que los servidores detrás del firewall no estén al alcance de atacantes externos y que puertos abiertos en servidores por descuido de algún encargado se encuentre vulnerable.

Para cumplir con las políticas básicas de firewall se describe los requerimientos necesarios y las herramientas utilizadas del software para cumplir con cada una de ellas:

Gestión de incidentes en la seguridad de la información

Para esta porción el software endian seleccionado tiene las siguientes herramientas que permiten presentar un informe detallado en tiempo real de las amenazas o incidentes en la seguridad como se observa en la Figura 22, esta sección se encuentra en la porción de registros e informes y permite visualizar en tiempo real el funcionamiento del firewall.

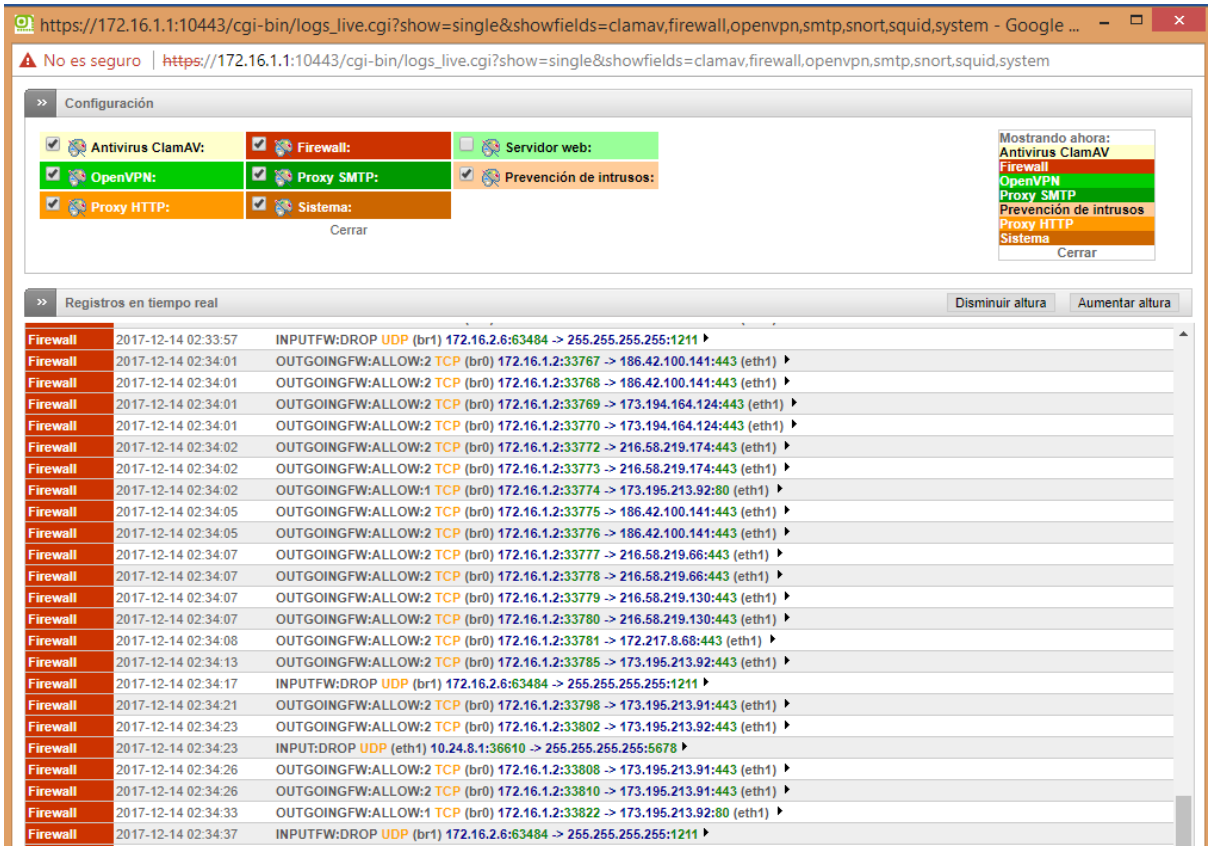


Figura 22. Reporte de incidentes en tiempo real
Fuente: Realizado por el autor

Como se puede observar en funcionalidad del software se pasa a comprobar la existencia de los reportes de eventos, reporte de debilidades, recolección de evidencia que son los parámetros que se dejaron mencionados para previamente comprobar su control por medio de la utilización de Endian.

Aprendizaje de los incidentes en la seguridad de la información**:** El software tiene un sistema de autoaprendizaje de Spam en caso de contar con un servidor de correo integrado en la infraestructura como se puede observar en la Figura 23.

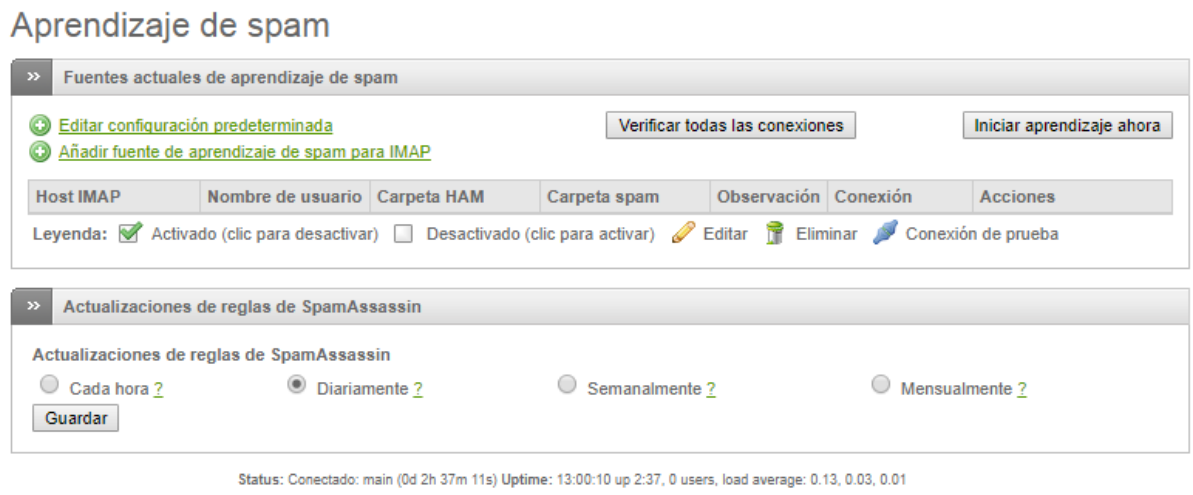


Figura 23. Autoaprendizaje spam
Fuente: Elaborado por el autor

Gestión de comunicaciones y operaciones

Para el cumplimiento de este objetivo de control en los parámetros mencionados como características funcionales a cumplir con el firewall se destaca lo siguiente:

Gestión de capacidad: Se deben controlar los cambios en los medios, por medio del sistema de monitorización NTOP integrado en Endian es posible controlar los cambios que se producen en la red de datos, como se puede observar en la Figura 24.

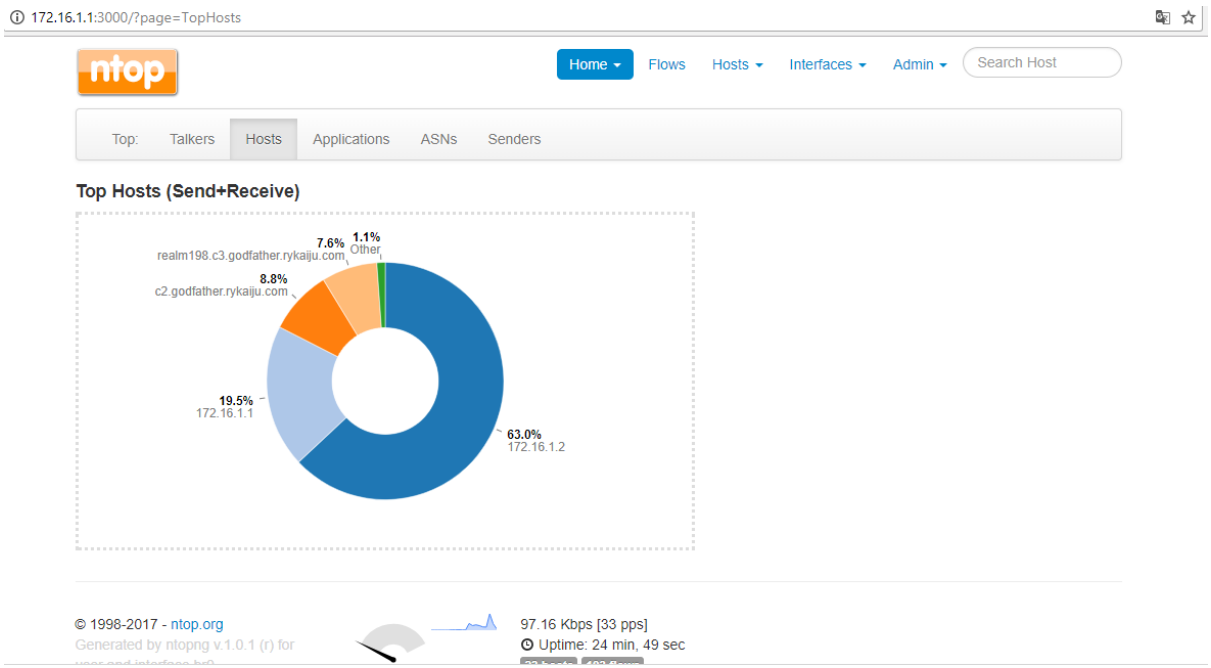


Figura 24. Sistema de monitorización NTOP
Fuente: Realizado por el autor

Controles de software malicioso: Para el cumplimiento de este objetivo de control el software Endian presenta un sistema antivirus integrado en las comunicaciones con una base de firmas de detección que se configura para su funcionamiento como se puede observar en la Figura 25.

Figura 25. Configuración Antivirus en Endian
Figura: Realizada por el autor

Controles de red: Para este apartado es importante destacar que Endian se encarga de separar las redes de manera eficiente, al asignar redes y reglas de acceso por defecto entre WAN, DMZ, LAN y red Wireless.

El software integra todos los controles necesarios para separar las redes y controladas por medio del sistema de reportes en tiempo real y el sistema de monitorización detallados en la Figura 21 y Figura 22 respectivamente.

Seguridad de los servicios de red: Para este control es necesario establecer políticas que permitan restringir los niveles de acceso a los servidores integrados en el Data-Center, actualmente se puede encontrar los servidores y servicios integrados en la red con los puertos necesarios para su acceso como se puede observar en la Tabla 33.

Tabla 33.
Dirección y Puertos en la DMZ

Servicio	**Dirección IP**	**Puerto**	
Openstack	172.16.2.17	http	80
Modle/ Repositorios	172.17.2.7	http	80
Opina/Reactivos	172.17.2.15	http	80
Voz/Ip	172.17.2.3	SIP RTP	5060 10000:20000

Fuente: Realizados por el autor

Para generar el acceso a los servidores integrados es necesario realizar la redirección de puertos como se observa en la Figura 26.

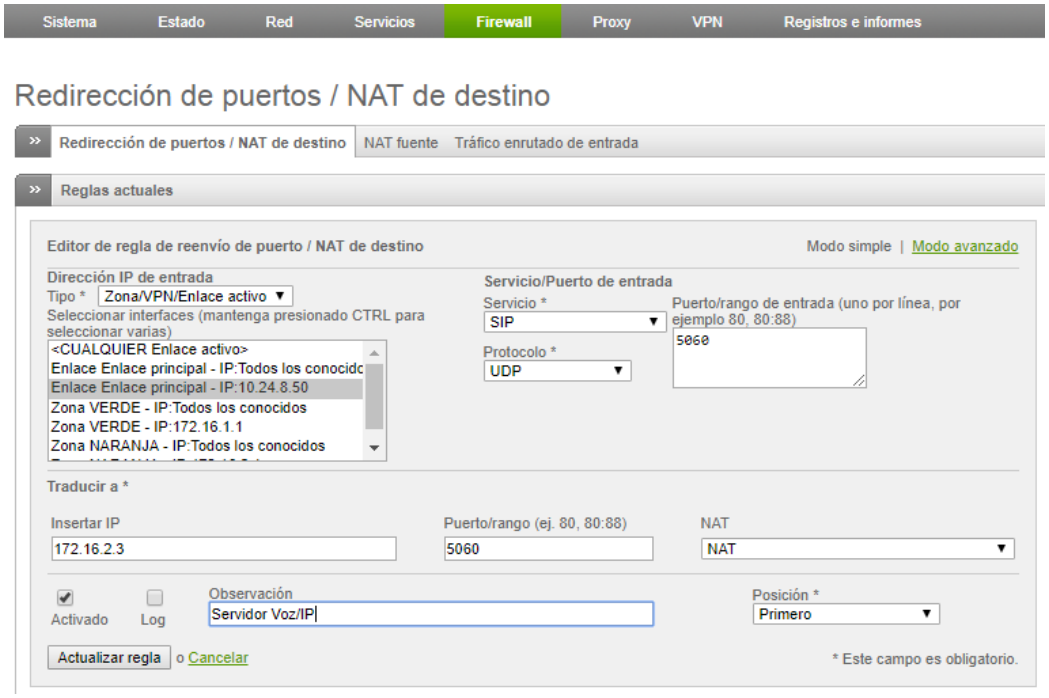


Figura 26. Configuración NAT acceso DMZ
Fuente: Realizado por el autor

Al final se integrarán los servidores que actualmente se encuentran activos generando las políticas de acceso como se puede ver en la Figura 27, el procedimiento se repite y se asigna uno a uno los servidores al enlace red para su visualización por la internet por medio de la ip publica provista por el DDTI.

Figura 27. Reglas NAT DMZ acceso externo
Fuente: Realizado por el autor.

En caso de ser necesario agregar un servicio nuevo en el Data-Center el encargado deberá realizar una solicitud al administrador del Data-Center indicando la dirección IP dentro de la DMZ y el puerto o puertos utilizados por el servidor.

Control de acceso

Autenticación del usuario para conexiones internas: Cada servidor cuenta con un proceso de autenticación del servicio al menos para la parte administrable que se encarga de modificar los servicios, además que se puede generar una regla mediante firewall para que solo el administrador de red por medio de autenticación MAC como se ve en la figura 28 pueda acceder al interfaz de Endian por medio de la regla establecida en la Figura 29.

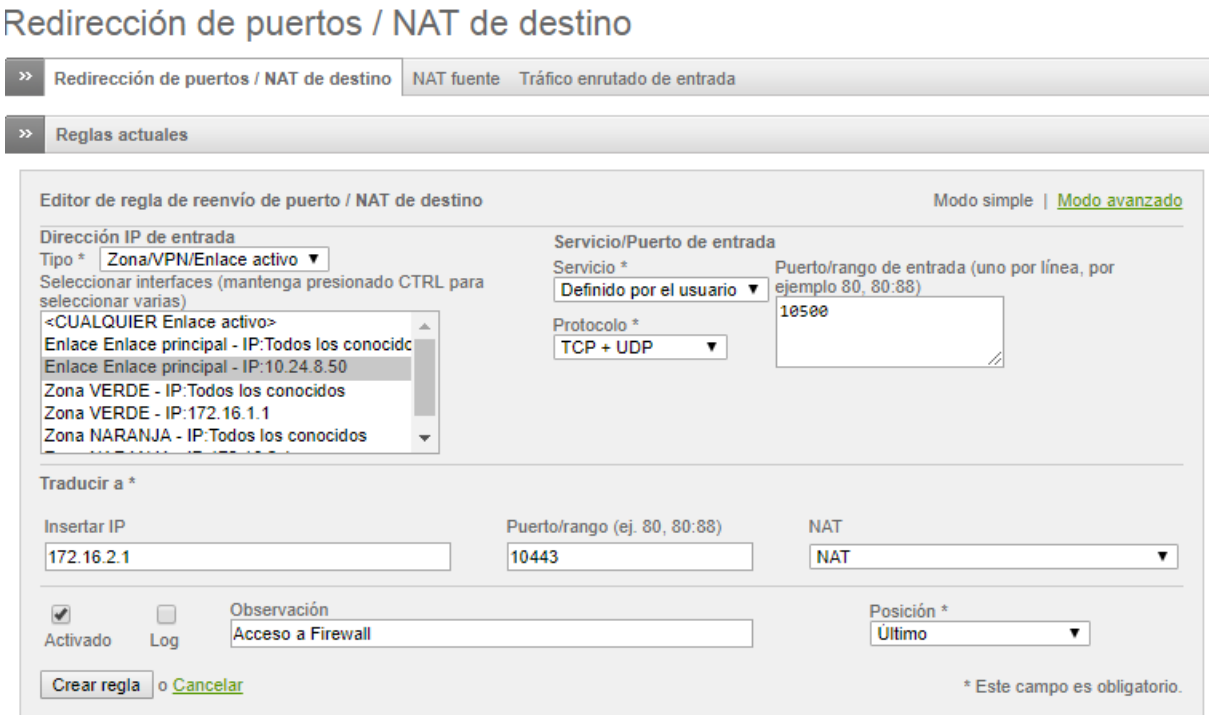


Figura 28. Acceso externo a Endian
Fuente: Elaborado por el autor

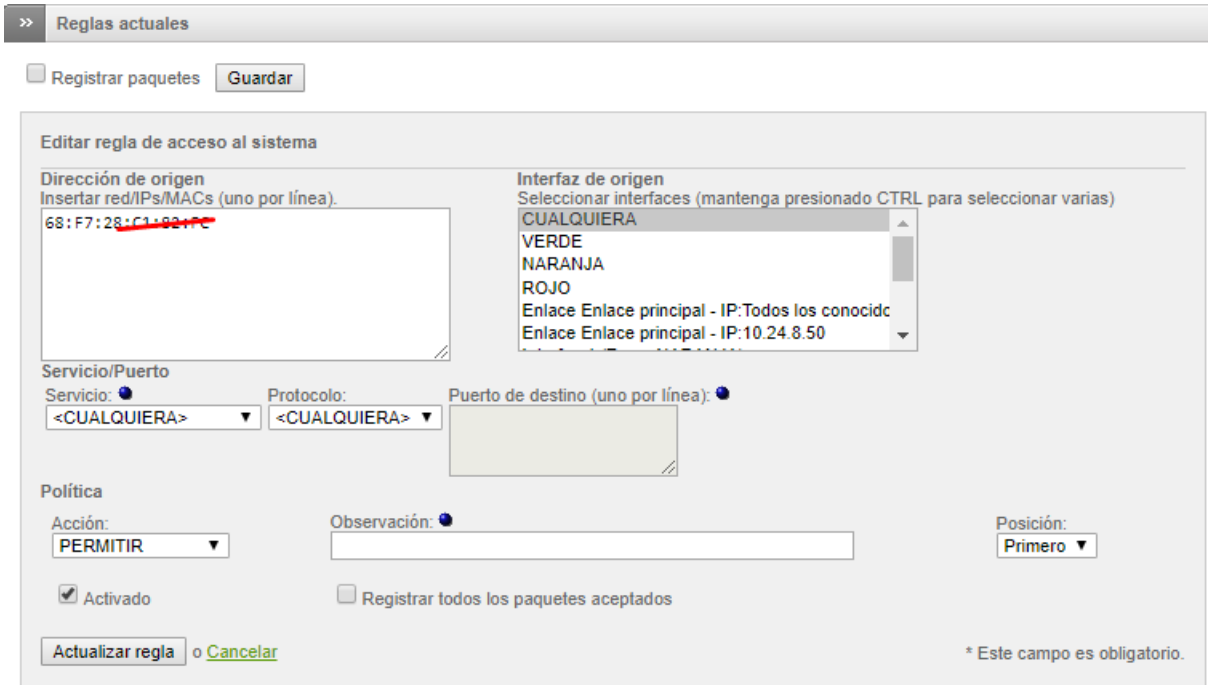


Figura 29. Configuración MAC para acceso a Endian
Fuente: Elaborado por el autor

Identificación de equipo en la red: En base al sistema integrado dentro de Endian por medio de su puerto 3000 se puede acceder a NTOP en donde cada usuario que accede a la red o la integra esta monitorizado, además se crearon las fichas técnicas referenciadas en el Anexo 2 que identifican a los servidores integrados en el Data-Center.

En la Figura 30 se puede observar los hosts que se conectan por medio del firewall y el sistema de monitorización.

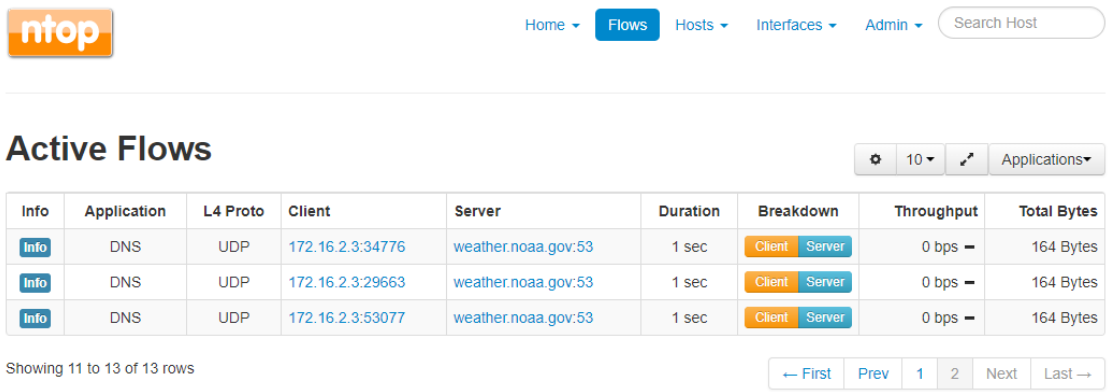


Figura 30. Estado de los hosts en la red
Fuente: Elaborado por el autor

Segregación de la red: En base a lo expuesto en las características del software la red se mantiene segregada por medio de la utilización de las propias características de Endian por la cual delimita cada una de las redes creadas en este caso la DMZ de la WAN.

Aislamiento de la información sensible: Los servidores con información sensible se encuentran detrás del firewall en la DMZ con una regla de acceso restringido solo habilitado los puertos para brindar los servicios necesarios a los usuarios finales pero el acceso a las plataformas como administrador está restringida por medio contraseñas propias de cada servidor y un bloqueo por parte del firewall solo habilitado en caso de requerirse el acceso externo.

- Autenticación del usuario para conexiones externas
- Identificación del equipo en red
- Protección del puerto de diagnóstico remoto
- Segregación en redes
- Control de conexión
- Limitación de tiempo de conexión
- Restricción al acceso a la información
- Aislamiento del sistema sensible

4.3. Resumen de políticas implementadas

Para desglosar toda la información expuesta se realiza un resumen de cada una de las políticas con su respectiva herramienta implementada. Todo se encuentra en la Tabla 34, Tabla 35, Tabla 36, Tabla 37, Tabla 38 y Tabla 39 respectivamente.

Tabla 34.
Políticas de seguridad de la información con su herramienta

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
Política	**Procedimiento**	**Herramienta**
Documentar la política de seguridad de información	Manual	Se elaboro unas políticas documentadas en el Anexo 12

Fuente: Elaborada por el autor

Tabla 35.
Organización de seguridad de la información con sus herramientas

ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
Política	**Procedimiento**	**Herramienta**
Coordinación de la seguridad de la información	Procedimental	Se tiene la elaboración de un diagrama de procedimiento para su cumplimiento referenciado en la Figura 12
Asignación de responsabilidades de la seguridad de la información	Procedimental	La estructura organizacional es descentralizada, mantiene un administrador de red y encargados directos de cada servidor, por lo cual las responsabilidades son asignadas por el administrador de red
Proceso de autorización para los medios de procesamiento de información	Procedimental	Procedimiento Figura 13
Contacto con autoridades	Administrativo	El contacto se realizará por parte de los encargados de cada servidor con el administrador de red
Contacto con grupos de interés	Administrativo	El administrador de red debe incentivar las relaciones con grupos externos.
Revisión independiente de la seguridad de la información	Administrativo	El administrador identificara las necesidades que no se pueden complementar de manera interna y se procede a utilizar los convenios realizados para solicitar colaboración en auditorias independientes.

Fuente: Elaborada por el autor

Tabla 36.
Gestión de Activos con su herramienta

GESTIÓN DE ACTIVOS		
Política	**Procedimiento**	**Herramienta**
Inventario de Activos Propiedad de los activos Uso aceptable de los activos Lineamientos de clasificación Etiquetado y manejo de información	Manual	Es importante destacar que para el cumplimiento de este objetivo de control se encuentran las fichas técnicas de los servidores referenciadas en el Anexo 2

Fuente: Elaborada por el autor

Tabla 37.
Gestión de comunicaciones y operaciones

GESTIÓN DE COMUNICACIONES Y OPERACIONES		
Política	**Procedimiento**	**Herramienta**
Procedimientos de operación documentados Gestión del cambio Segregación de deberes Separación de los medios de desarrollo y operacionales Aceptación del sistema	Procedimental	Formato de procedimientos Anexo 14. Procedimiento en la Figura 14
Gestión de los medios removibles Eliminación de medios Seguridad de la documentación del sistema	Procedimental	Procedimiento medios extraíbles Figura 15. Generación Formal Políticas Anexo 12
Gestión de capacidad	Software	Endian Firewall por medio de su herramienta NTOP
Controles de software malicioso	Software	Endian Firewall sistema integrado antivirus ClamAV
Controles de red	Software	Endian Firewall con puente para separación de WAN y DMZ
Seguridad de los servicios de red	Software	Endian Firewall con todas las funcionalidades que presenta en la porción de firewall.

Fuente: Elaborada por el autor

Tabla 38.
Control de acceso con sus herramientas

CONTROL DE ACCESO		
Política	**Procedimiento**	**Herramienta**
Gestión de privilegios	Procedimental	Política generada Anexo 12
Gestión de la clave del usuario	Manual	Cada encargado se encarga de gestionar los usuarios y las claves que se manejaran por el servicio brindado.
Revisión de los derechos de acceso del usuario Uso de clave Política sobre el uso de servicios en red	Procedimental	Para cumplir con estos controles se generaron las políticas que están referenciadas en el Anexo 12.
Autenticación del usuario para conexiones externas	Software	Para este proceso se implementará Endian Firewall que permite realizar redireccionamiento NAT para acceder a los servidores que se encuentran en la DMZ permitiendo el acceso remoto, previo a esto cada servidor cuenta con una base de datos en mysql que controla los usuarios por medio de un interfaz propio independiente
Identificación del equipo en red	Software	Se utilizará una herramienta integrada en Endian Firewall que se denomina NTOP y permite visualizar los host o servidores con actividad en la red.

Protección del puerto de diagnóstico remoto	Software	Para el acceso remoto tanto a los servidores como el entorno Firewall se utilizará una autenticación por MAC.
Segregación en redes	Software	Endian Firewall se encargará de separar la red WAN de la DMZ para de esta forma proteger los servidores y la información que almacena.
Control de conexión	Software	Se utilizará NTOP que permite visualizar las conexiones activas además del monitoreo del firewall y conexiones en tiempo real que Endian integra.
Control de 'routing' de redes	Software	Endian Firewall se encarga de enrutar los paquetes y revisarlos mediante sus gestores de monitorización en tiempo real.
Procedimiento de registro en el terminal	Procedimental	El encargado de cada uno de los servidores tiene como obligación realizar la agregación de nuevos usuarios para el acceso y sus privilegios.
Identificación y autenticación del usuario	Administrativo	Cada servidor maneja su sistema autenticador propio por medio de una base de datos mysql encriptada. Además de la red inalámbrica posee un sistema de LDAP por medio de mikrotik y un switch de distribución que interconecta a unos AP que autentican e identifican cada usuario que accede por medio de la red inalámbrica
Sistema de gestión de claves	Manual	El sistema de claves se lo manejara por cada uno de los encargados, pero a su vez existe un formato manual para su elaboración
Limitación de tiempo de conexión	Software	Mediante la utilización de las seguridades presentadas por medio de Endian Firewall también integra el software o proxy squid para manejo de tiempos de acceso, pero al definirse como un sistema de red WAN y DMZ no se lo implemento por ser requerido para los servicios presentados.
Restricción al acceso a la información	Manual	Por medio de la política implementada los usuarios se manejan bajo estricto cumplimiento, además el administrador de la red debe encargarse de generar los acuerdos de confidencialidad.
Aislamiento del sistema sensible	Software	Se utiliza Endian Firewall para proteger la información de cada uno de los servidores que integran la infraestructura por medio de la creación de la DMZ

Fuente: Elaborada por el autor

Tabla 39.
Gestión de incidentes en la seguridad de la información con sus herramientas

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
Política	**Procedimiento**	**Herramienta**
Reporte de eventos en la seguridad de la información Reporte de debilidades en la seguridad Responsabilidad y procedimientos Recolección de evidencia	Software	Para el cumplimiento de esta política se utilizará Endian Firewall y su funcionalidad de reportes e informes.
Aprendizaje de los incidentes en la seguridad de la información	Software	Se utilizará Endian Firewall con sus dos funcionalidades las cuales son: Aprendizaje de Spam SNORT

Fuente: Elaborada por el autor

Capítulo V

Pruebas de Funcionamiento

Para cada uno de las herramientas implementadas se procede a realizar las pruebas de funcionamiento para el software implementado las cuales se resumirán en verificar el funcionamiento de los siguientes objetivos de control presentados en la Tabla 40.

Tabla 40.
Objetivos de Control Pruebas de Funcionamiento

Gestión de capacidad	Software	Endian Firewall por medio de su herramienta NTOP
Controles de software malicioso	Software	Endian Firewall sistema integrado antivirus ClamAV
Controles de red	Software	Endian Firewall con puente para separación de WAN y DMZ
Seguridad de los servicios de red	Software	Endian Firewall con todas las funcionalidades que presenta en la porción de firewall.

Fuente: Elaborada por el autor

Gestión de Capacidad: Para probar el funcionamiento de esta herramienta se procede a observar cada uno de los interfaces que permiten monitorizar las condiciones de la red implementada, como se puede observar en la parte de monitorización cada vez que un servidor está activo se puede observar su interacción en la red por medio de NTOP un software integrado en Endian. En la Figura 31 se puede observar un interfaz bastante amigable que permite observar las interacciones del software con los hosts que la conforman.

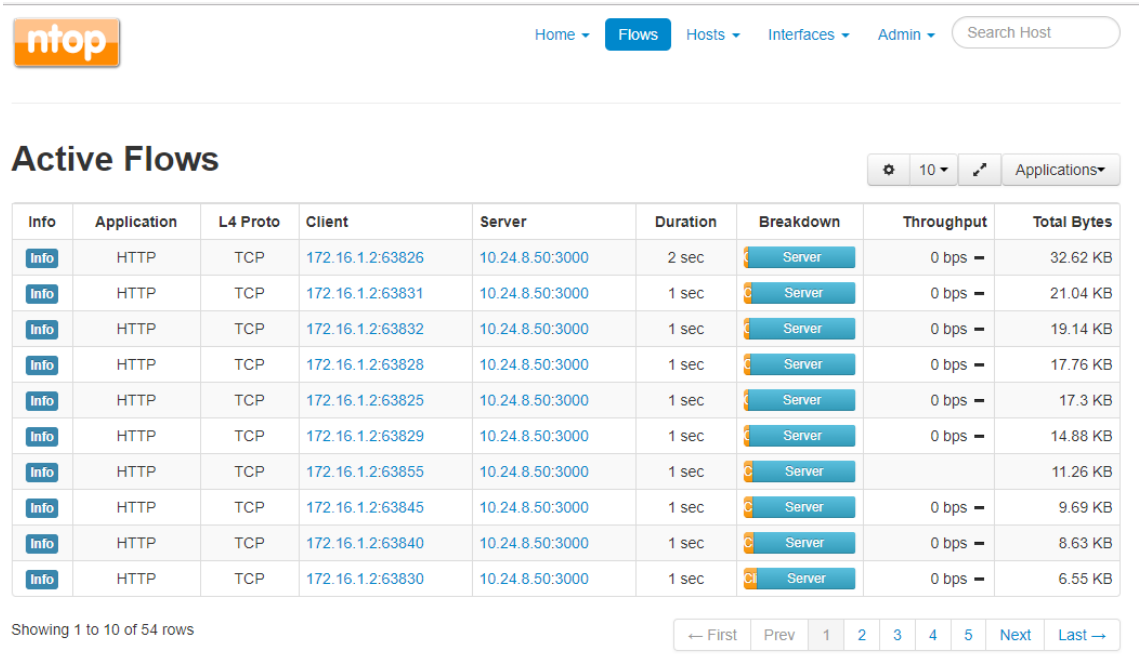


Figura 31. Monitorización de host y server activos NTOP
Fuente: Elaborada por el autor

Para visualizar de una manera más específica se selecciona un servidor dentro de la red, en la Figura 32 se puede visualizar los protocolos que maneja el servidor de voz ip que integra el centro de datos y que se asignó con la IP 172.16.2.3.

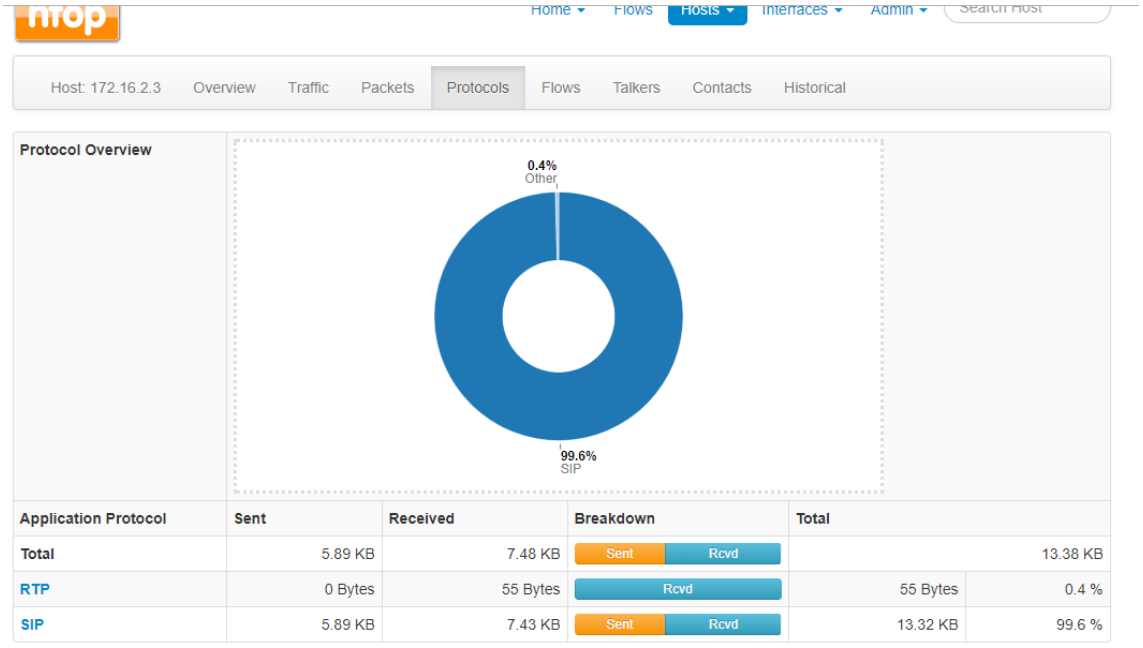


Figura 32. Visualización protocolos servidor voz/IP
Fuente: Elaborada por el autor

Además, es posible tener un conjunto de estadísticas diarias de la actividad del servidor y el tipo de datos que genera y recibe, en la Figura 33 se puede observar la actividad del servidor Moodle integrado en el Data-Center.

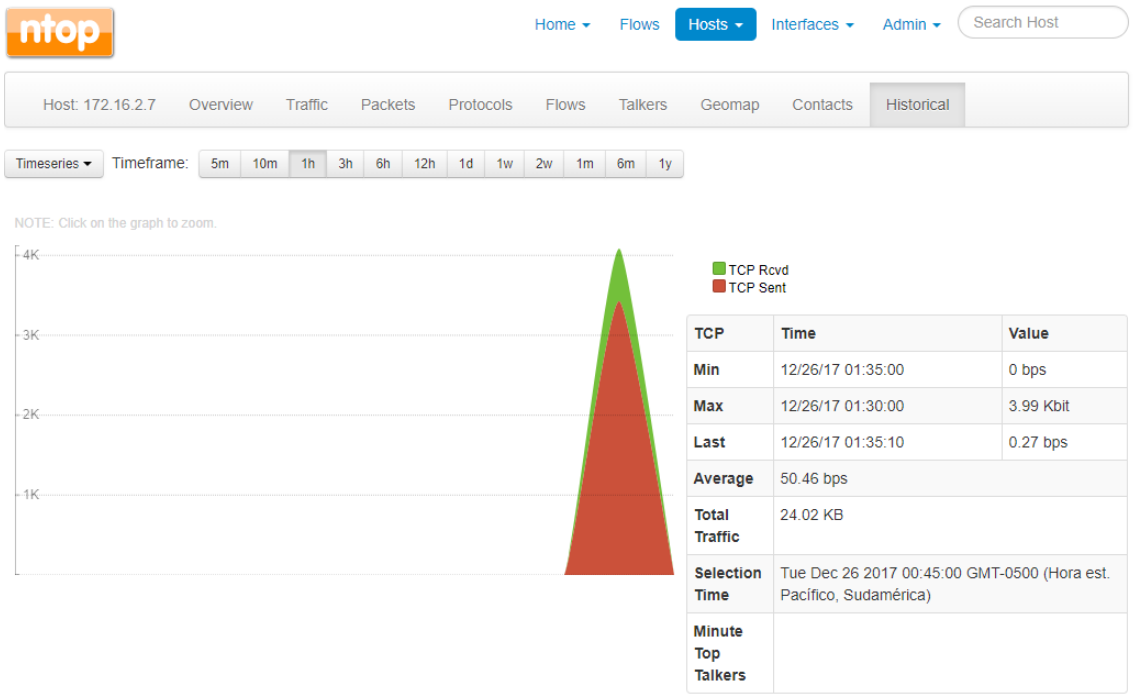


Figura 33. Revisión de Flujo de Paquetes en servidor Moodle
Fuente: Elaborada por el autor

Controles de software malicioso: Dentro del interfaz se puede encontrar la opción de utilizar un sistema antimalware llamado ClamAV el cual permite que los correos enviados a través de la infraestructura sean analizados en busca de spam, solo es cuestión de haberlos habilitado previamente. En la Figura 34 se puede observar el interfaz en su funcionamiento en caso de encontrar amenazas se tiene un reporte en tiempo real.

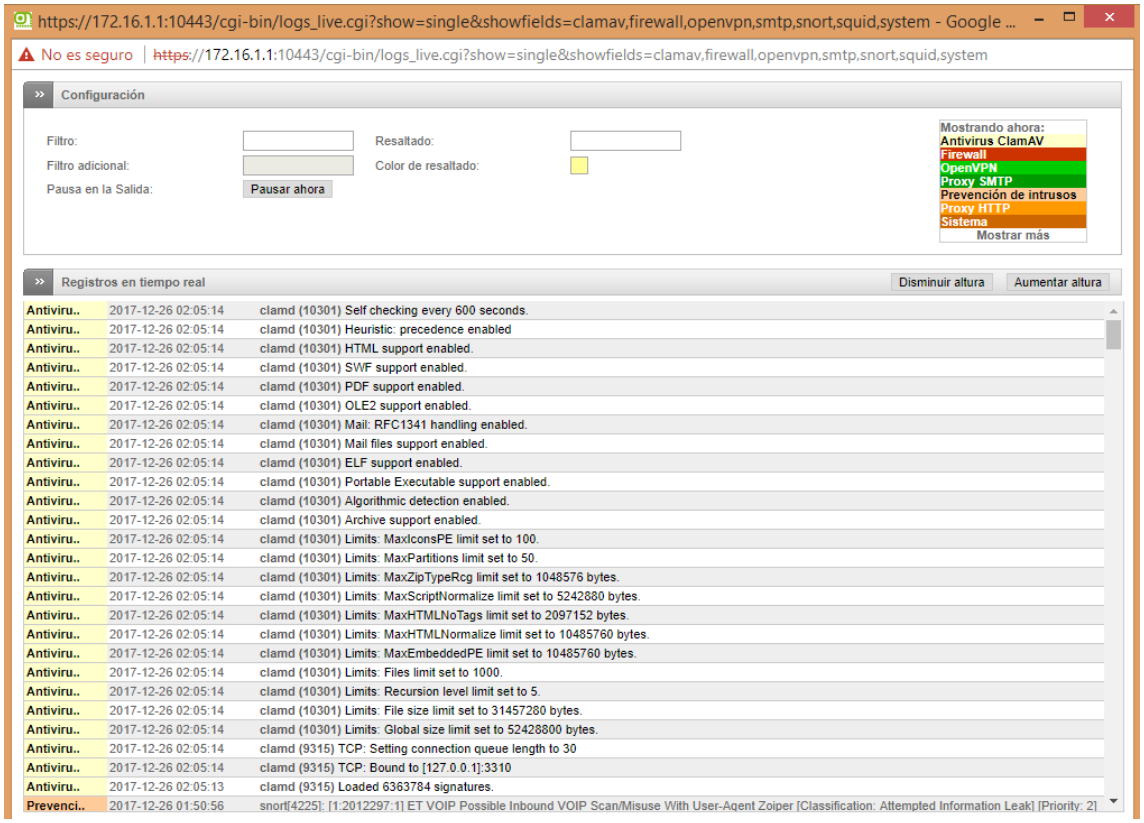


Figura 34. Visualización en tiempo real del software ClamAV
Fuente: Elaborada por el autor

Seguridad de los servicios de red: Dentro de las funcionalidades de Endian existe la separación de redes permitiendo que la DMZ, encargada de alojar los servidores y servicios se mantenga aislada de intrusión externa no permitida, por medio de la implementación de una política de denegar todo, de esta manera solo se habilita el acceso al puerto y dirección IP específica del servicio. Así se rechaza o deniega el resto de puertos y protocolos que se puedan encontrar activos por fallas de configuración. En la Figura 35 se puede observar las reglas de acceso del firewall, mientras en la Figura 36 se puede visualizar en tiempo real el bloqueo de accesos no deseados a la infraestructura.

Reglas actuales

Agregar nueva regla de reenvío de puerto / NAT de destino

#	Dirección IP de entrada	Servicio	Política	Traducir a	Observación	Acciones
1	10.24.8.50 (Enlace main)	UDP/5060		172.16.2.3 : 5060	Servidor Voz/IP	
	PERMITIR con IP desde:			<CUALQUIERA>		
2	10.24.8.50 (Enlace main)	TCP/8081		172.16.2.7 : 80	Moodle	
3	10.24.8.50 (Enlace main)	TCP+UDP/8084		172.16.2.15 : 80	Openstack	
	PERMITIR con IP desde:			<CUALQUIERA>		
4	10.24.8.50 (Enlace main)	TCP/20 TCP/21		172.16.2.7 : 20:21	Repositorios	
5	10.24.8.50 (Enlace main)	TCP+UDP/1024		172.16.2.15 : 80	Opina	
6	10.24.8.50 (Enlace main)	TCP+UDP/35		172.16.2.7 : 22	Moodle Acceso SSH	
7	10.24.8.50 (Enlace main)	TCP+UDP/443		172.16.2.1 : 10443	Acceso a Firewall	

Figura 35. Reglas de acceso en el Firewall
Fuente: Elaborada por el autor

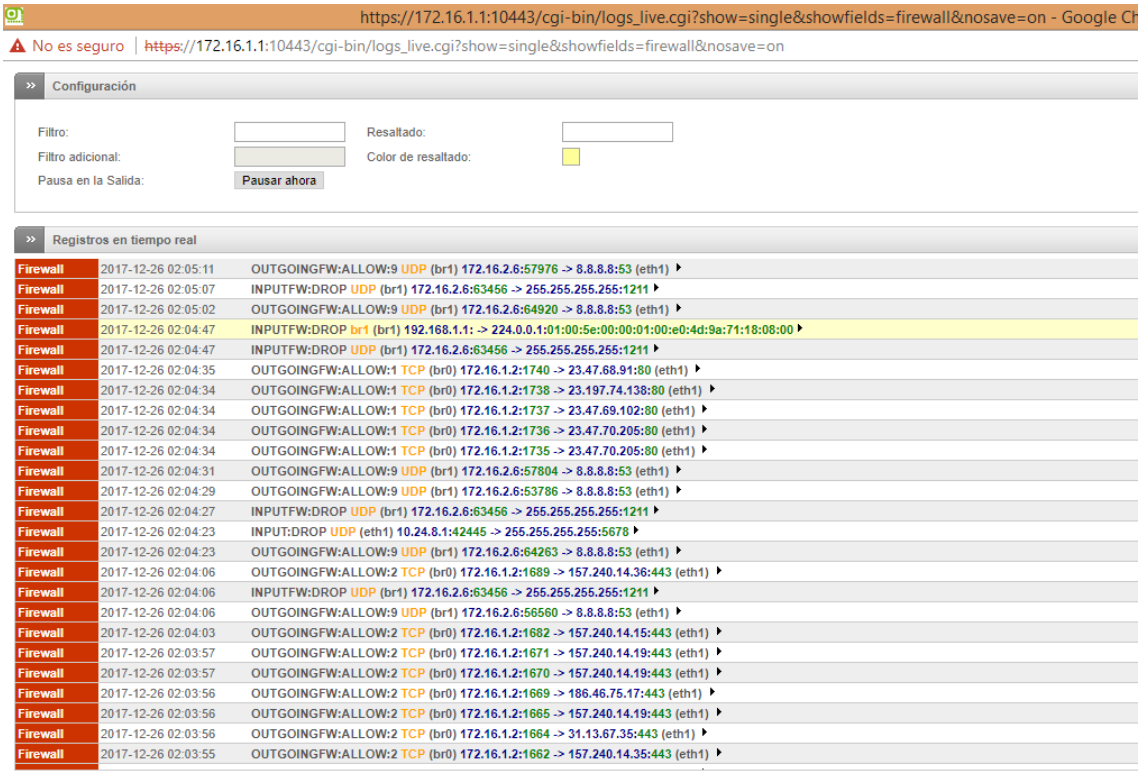


Figura 36. Visualización Reglas Firewall en tiempo real
Fuente: Elaborada por el autor

Como se puede observar en las pruebas se realizó una solicitud por medio de ICMP que indica que el acceso para puertos que no se encuentran habilitados y están bloqueados por medio de Endian, se bloqueó tanto el acceso de los servidores para la realización de peticiones ICMP tanto a la WAN como a la DMZ.

En la Figura 37 se puede observar la solicitud de ICMP hacia la WAN, y se puede observar que por medio de firewall se puede bloquear.

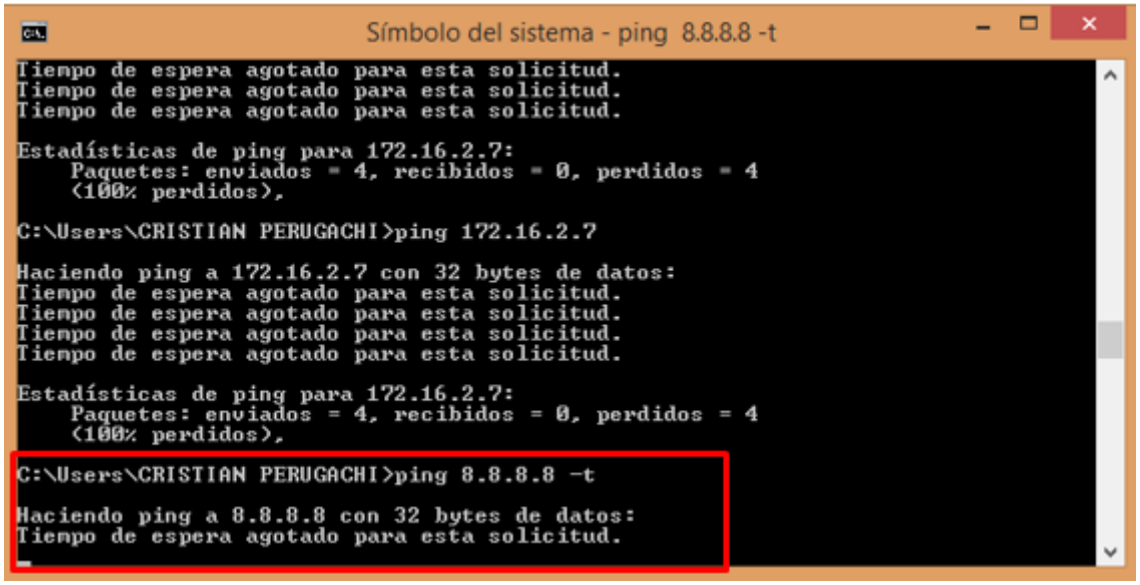


Figura 37. ICMP desde DMZ hacia WAN
Fuente: Elaborada por el autor

En la Figura 38 se puede observar la solicitud de ICMP hacia la DMZ, y se puede observar que por medio de firewall se está rechazando la solicitud al servidor moodle.

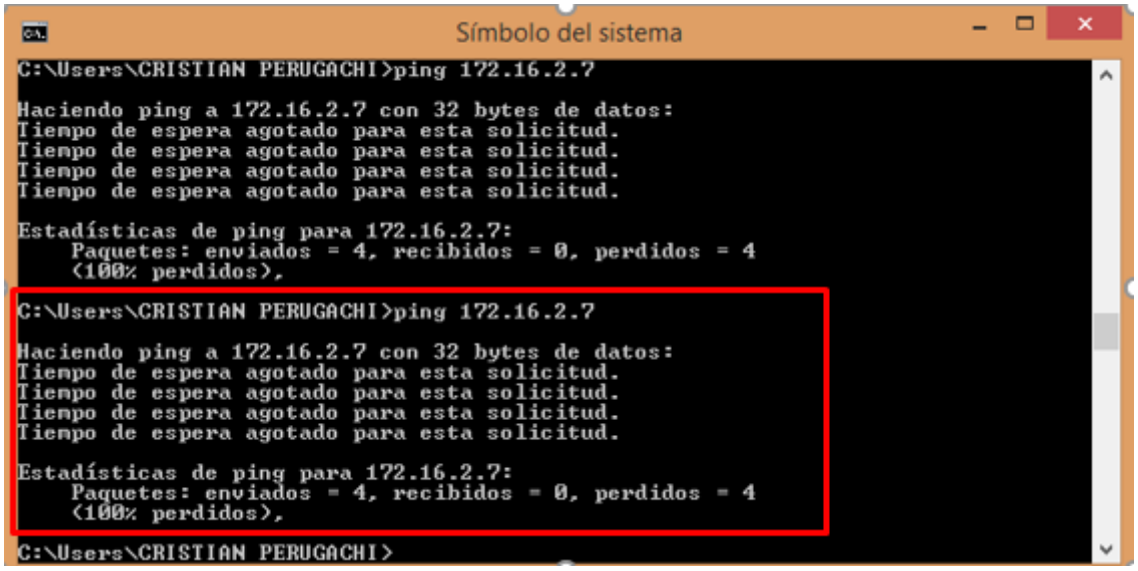


Figura 38. ICMP hacia la DMZ
Fuente: Elaborada por el autor

Autenticación del usuario para conexiones externas: Para probar el funcionamiento es necesario acceder mediante las reglas implementadas en endian firewall la porción de NAT que permite redireccionar la red WAN hacia la DMZ para acceso externo de los equipos, todas

las reglas implementadas en esa porción están referenciadas en la Figura 33, dentro de las pruebas a realizar se procede a probar el acceso a Moodle por medio de la DMZ como se puede observar en la Figura 39.

Figura 39. Acceso por medio WAN a servidor Moodle
Fuente: Elaborada por el autor

En la Figura 40 se puede observar el acceso al servidor Openstack implementado en el servidor HP Proliant y el acceso por medio del puerto 8084 redireccionado en el NAT de Endian Firewall.

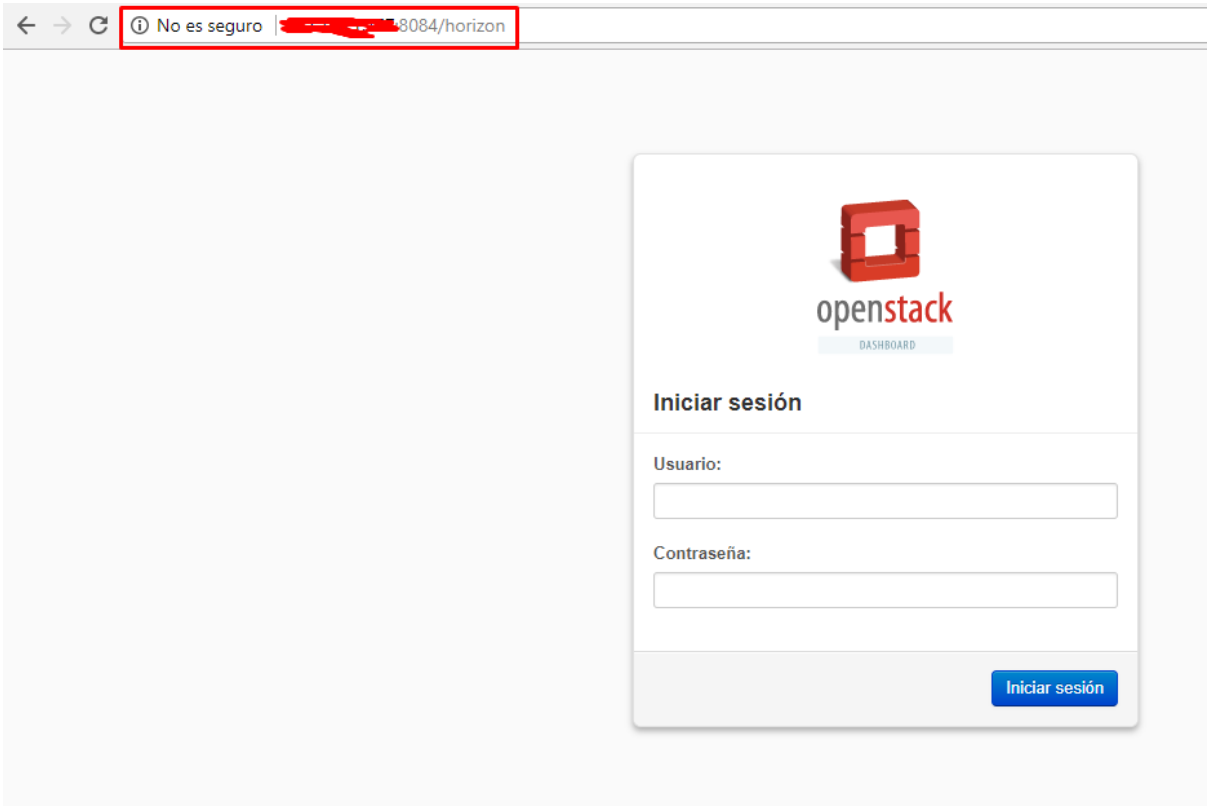


Figura 40. Acceso por medio de WAN a openstack
Fuente: Elaborada por el autor

En la Figura 41 se puede observar cómo se enlaza desde la WAN los usuarios de VOZ/IP y permiten el establecimiento de una llamada.

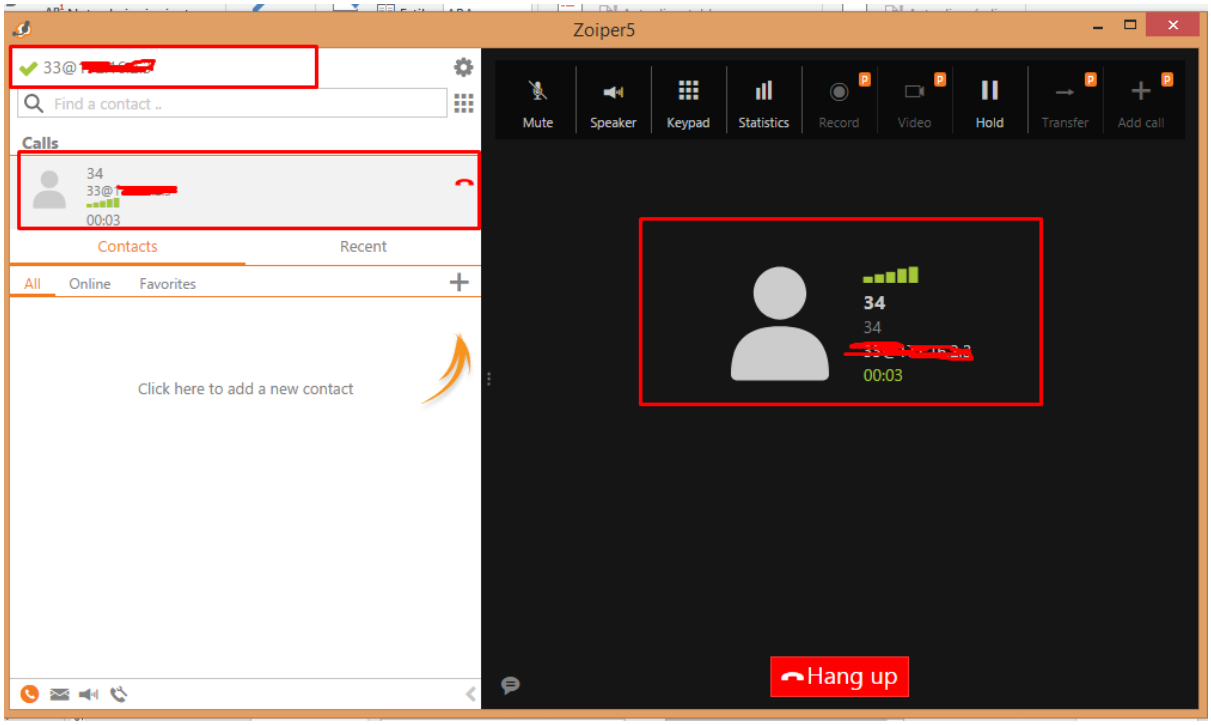


Figura 41. Acceso por medio de WAN a servidor VOZ/IP
Fuente: Elaborada por el autor

Identificación del equipo en la red: Para asegurar el funcionamiento es cuestión de revisar en el monitorizador de cada host que se encuentra como funcionalidad de Endian Firewall y se denomina NTOP, para lo cual es imperativo visualizar el servidor de VOZ/IP, servidor moodle y servidor openstack que se encuentran visualizados en la Figura 42, Figura 43 y Figura 44 respectivamente.

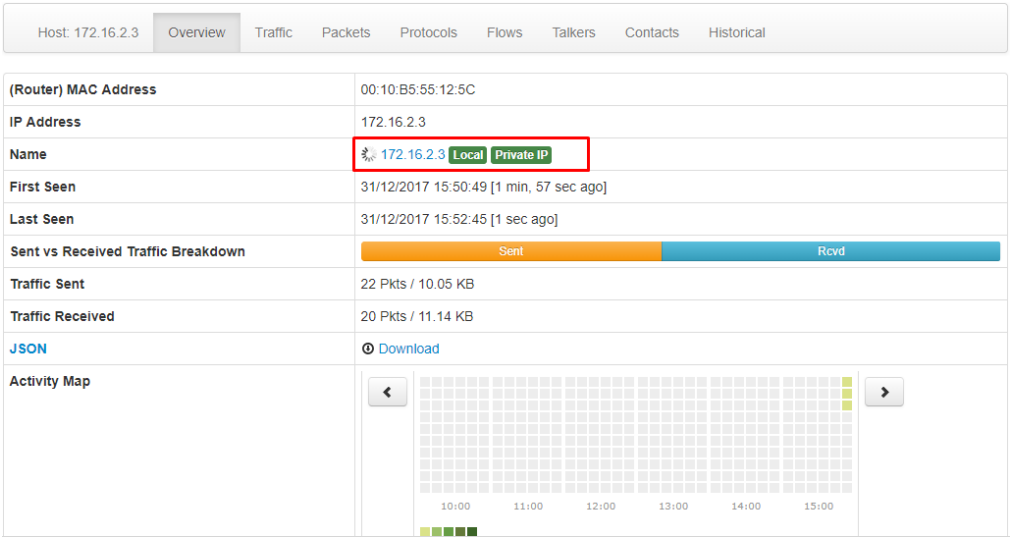


Figura 42. Servidor VOZ/IP visualizado en NTOP
Fuente: Elaborada por el autor

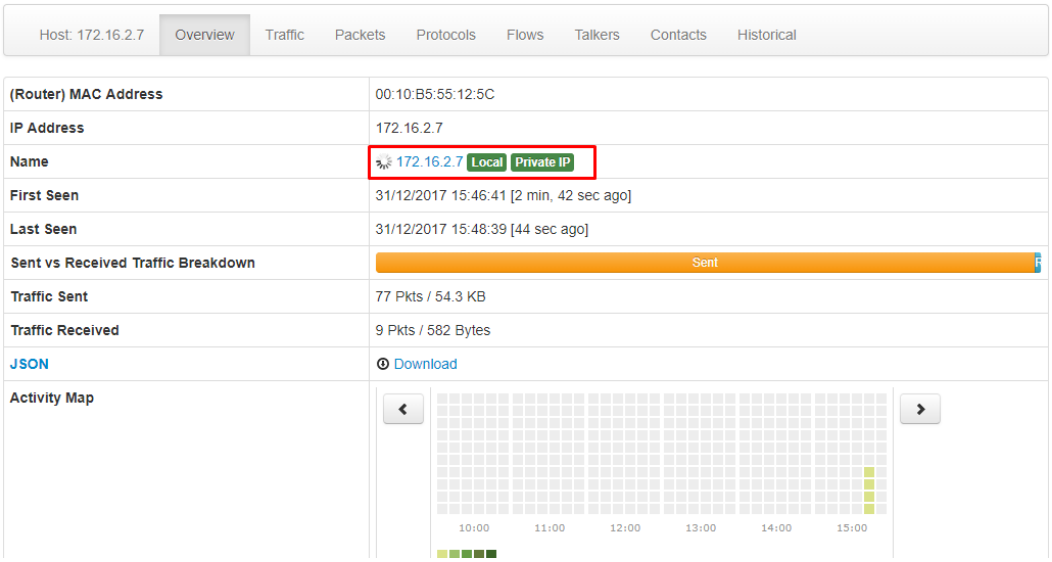


Figura 43. Servidor Moodle visualizado en NTOP
Fuente: Elaborada por el autor

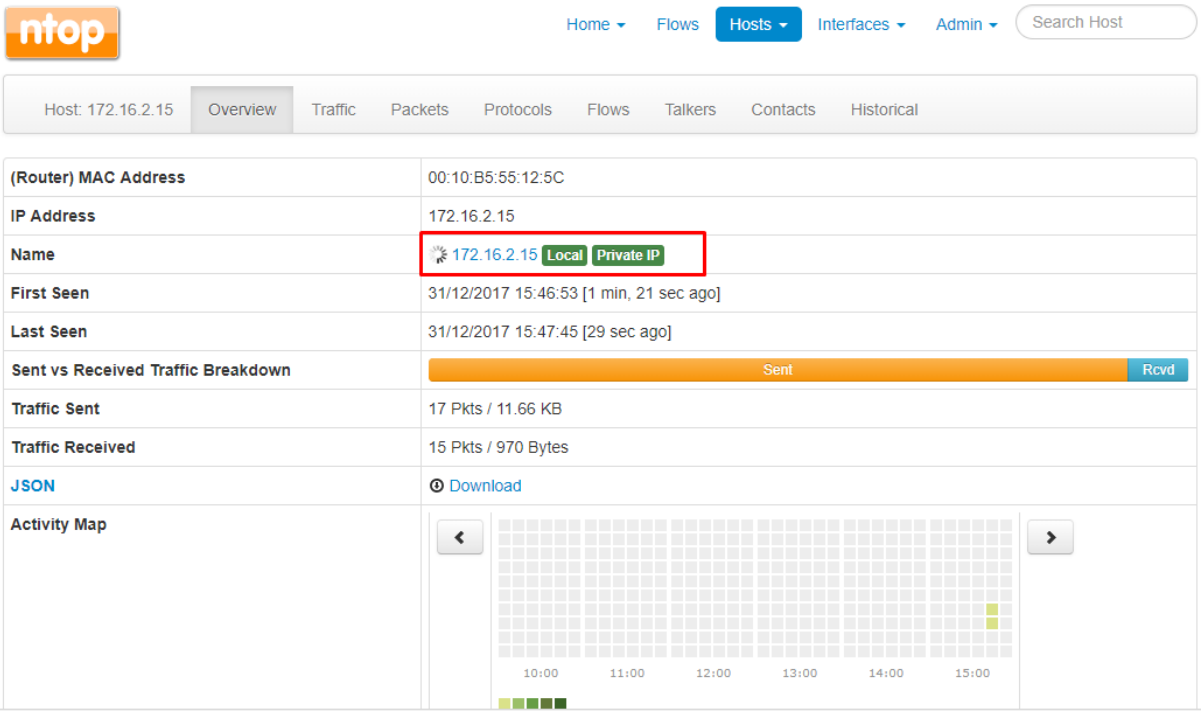


Figura 44. Servidor Openstack visualizado en NTOP
Fuente: Elaborada por el autor

Protección del puerto de diagnóstico remoto: El software Endian Firewall permite crear reglas personalizadas para que cada uno de los servidores integrados aseguren su conexión remota por SSH, como se puede observar en la Figura 45 que se ha realizado el NAT del servidor Moodle para su puerto remoto y acceso WAN.

Figura 45. Permitir Acceso SSH por IP
Fuente: Elaborada por el autor

Con esta regla se asegura que solo la persona que se ubique la IP especifica pueda acceder a SSH para el servidor Moodle que para la situación expuesta se trata del encargado del equipo, además es imperativo la negación del resto de direcciones IP para que nadie excepto el tenga permiso de acceso como se observa en la Figura 46.

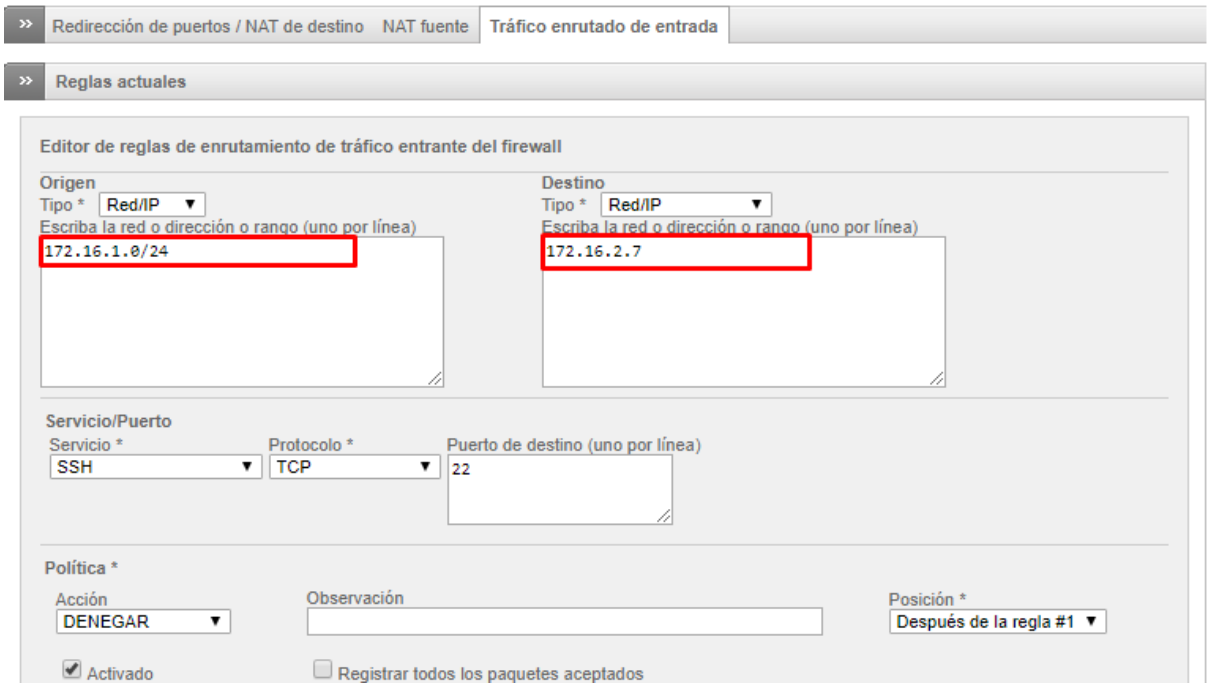


Figura 46. Denegación toda la porción de red para SSH
Fuente: Elaborada por el autor

Una vez realizado las configuraciones es importante elaborar las pruebas de funcionamiento por medio de Putty se procede a usar cualquier dirección IP como se observa en la Figura 47 para acceder por medio de SSH y el resultado se puede visualizar en la Figura 48.

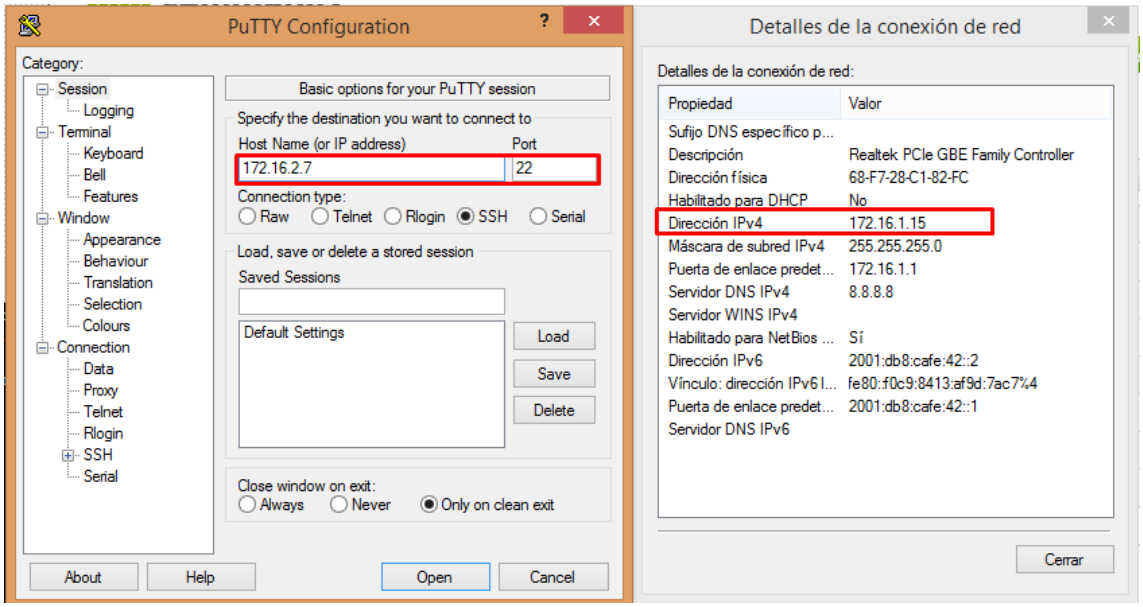


Figura 47. Configuración IP para acceso SSH por medio de Putty servidor Moodle
Fuente: Elaborada por el autor

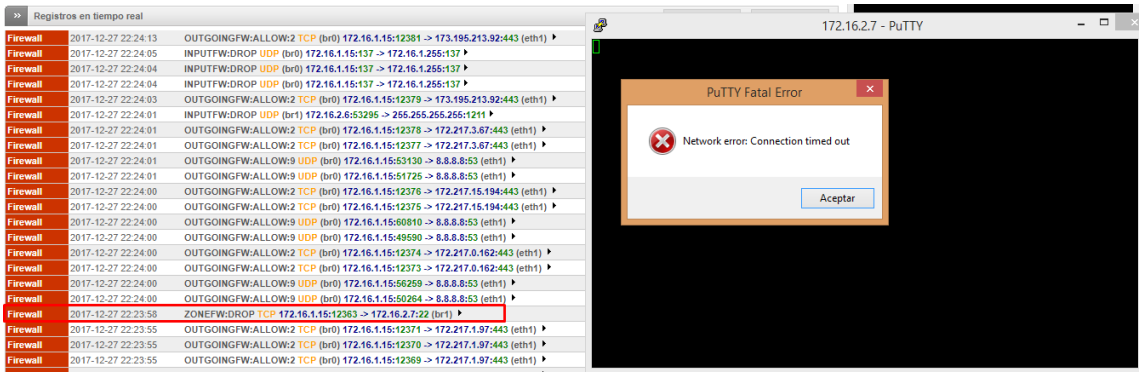


Figura 48. Denegación de acceso a SSH dentro del Firewall y bloqueo en Putty
Fuente: Elaborada por el autor

Para comprobar que se encuentra funcionando se procede con la asignación de la dirección IP permitida como se observa en la Figura 49, y el resultado o acceso se puede visualizar en la Figura 50.

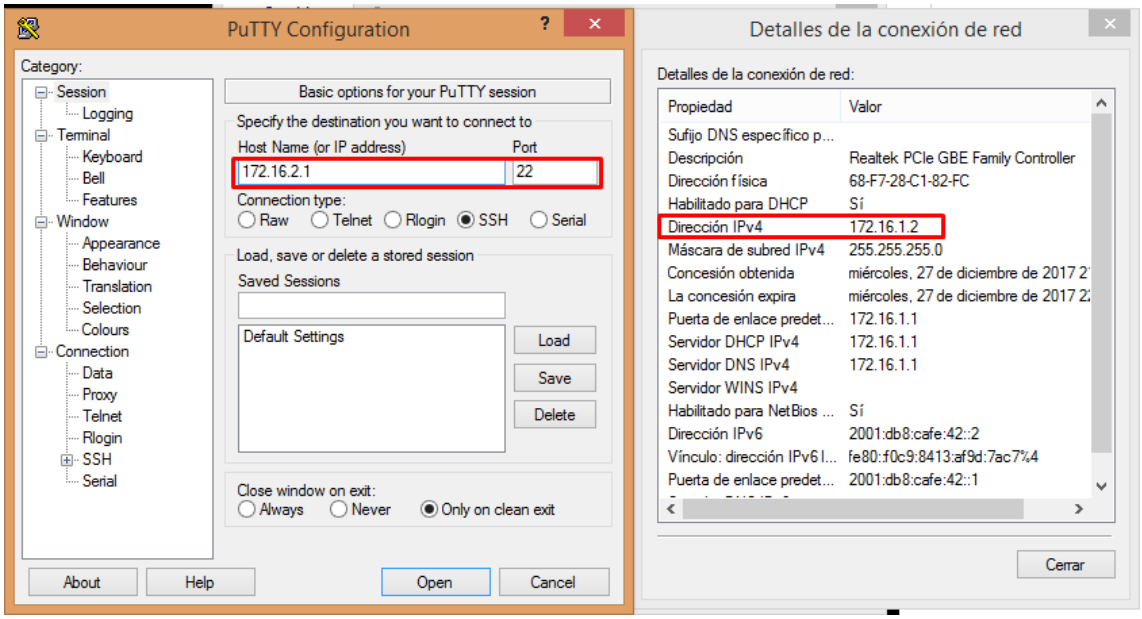


Figura 49. Asignación IP de administrador de servidor para acceso SSH mediante Putty
Fuente: Elaborada por el autor

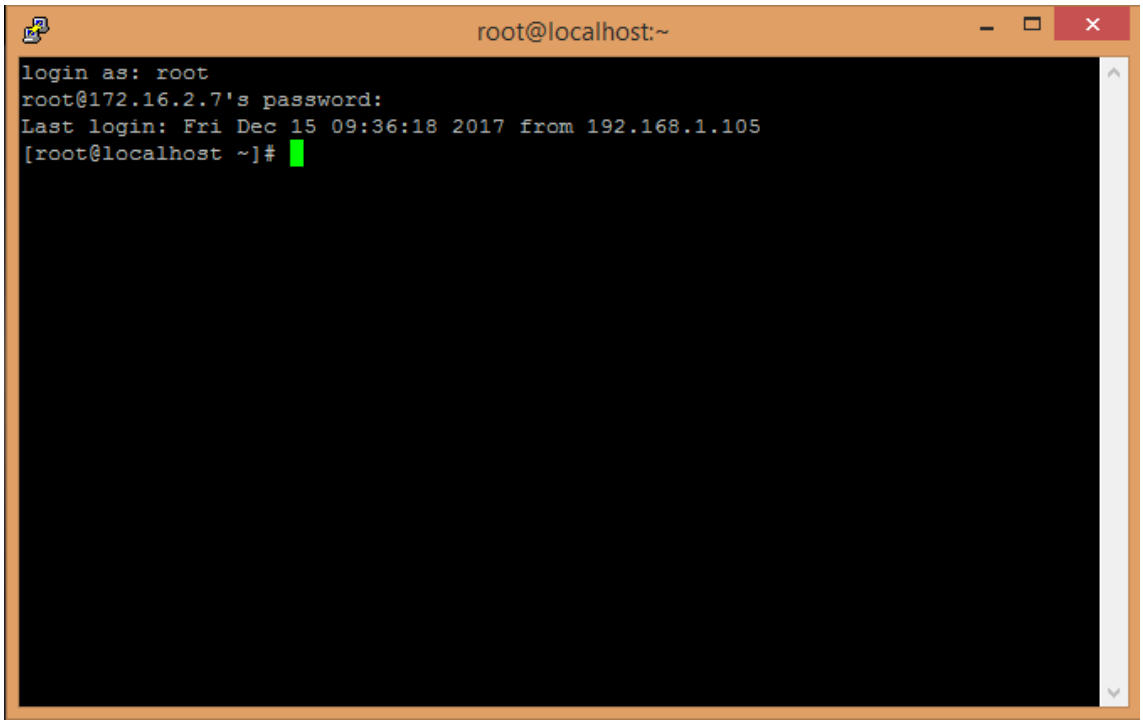


Figura 50. Acceso SSH aceptado
Fuente: Elaborada por el autor

Segregación de redes: El software Endian Firewall permite separar las redes en WAN, DMZ, LAN e Inalámbrica, cada una viene predeterminada con sus protecciones por defecto. En el caso presentado solo se requiere separar la WAN de la red DMZ donde se alojan los servidores, en la Figura 51 se puede encontrar las redes que se encuentran funcionando actualmente en el firewall.

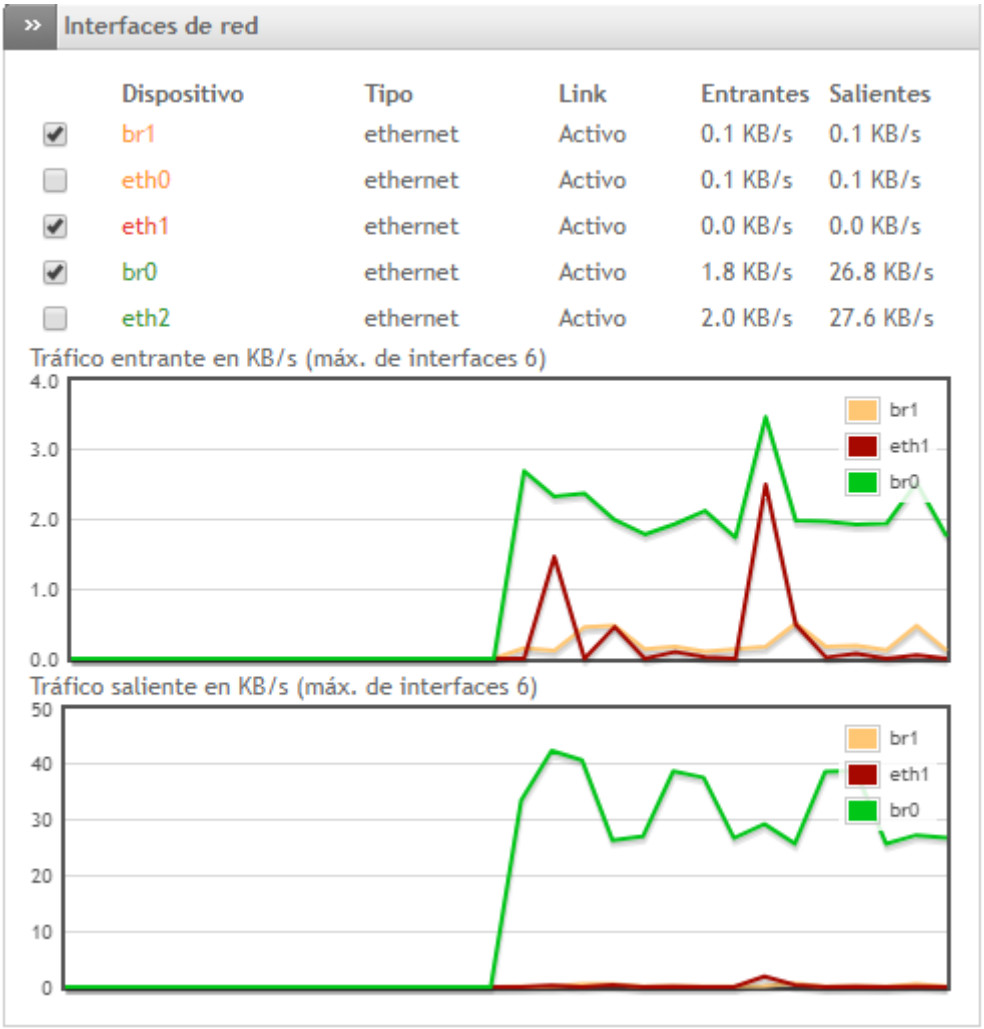


Figura 51. Redes Activas en el software firewall Endian
Fuente: Elaborada por el autor

Control de conexión: Dentro de la funcionalidad de NTOP implementada en Endian Firewall es posible visualizar en tiempo real todas las conexiones como se puede observar en la Figura 52.

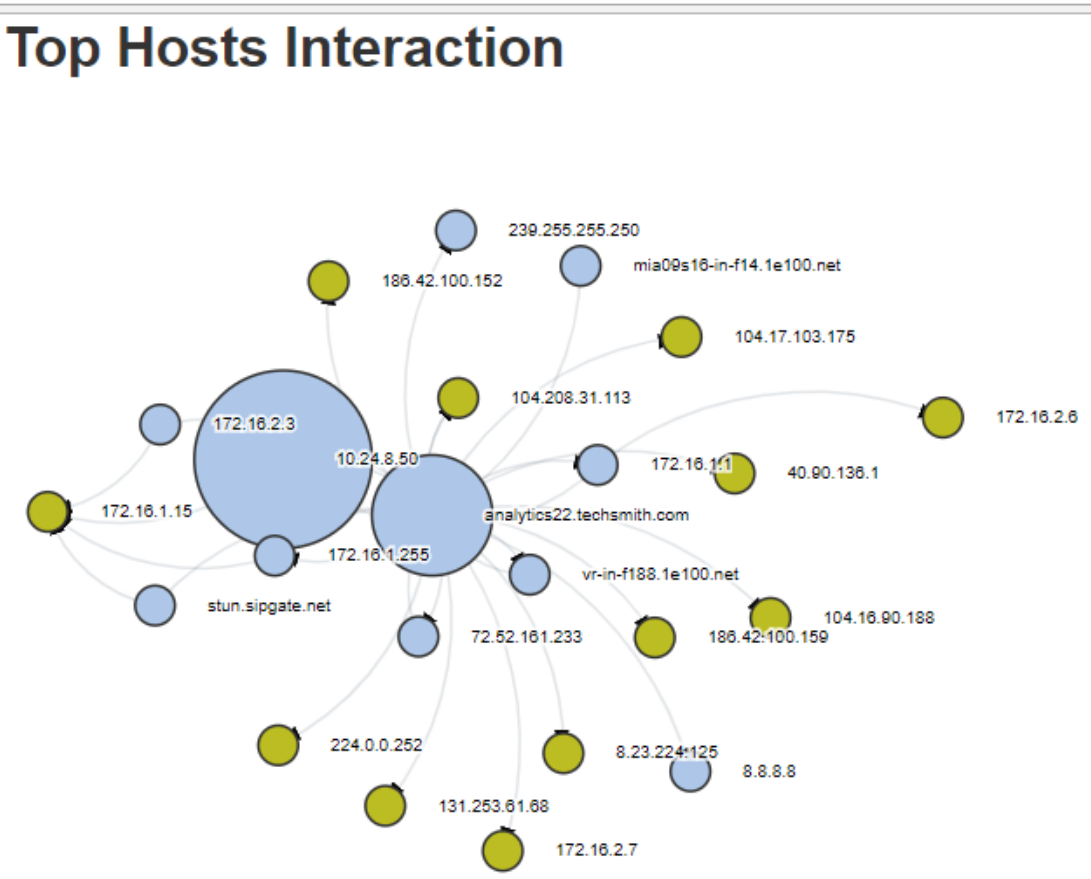
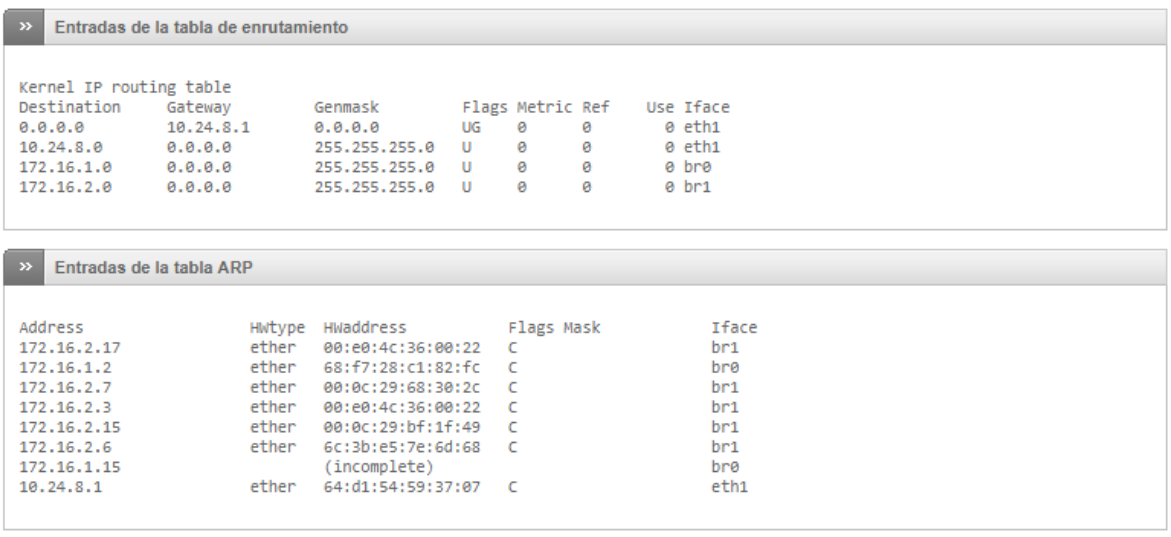


Figura 52. Visualización de Host activos en tiempo real de la Red
Fuente: Elaborada por el autor

Control de routing de redes: Endian permite enrutar y crear sus propias tablas de routing como se puede observar en la Figura 53, cada regla de enrutamiento agregada en el firewall se agrega automáticamente, además que se actualiza constantemente.



» Entradas de la tabla de enrutamiento

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.24.8.1       0.0.0.0         UG    0      0        0 eth1
10.24.8.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
172.16.1.0      0.0.0.0         255.255.255.0   U     0      0        0 br0
172.16.2.0      0.0.0.0         255.255.255.0   U     0      0        0 br1
```

» Entradas de la tabla ARP

```
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.2.17              ether   00:e0:4c:36:00:22   C                     br1
172.16.1.2               ether   68:f7:28:c1:82:fc   C                     br0
172.16.2.7               ether   00:0c:29:68:30:2c   C                     br1
172.16.2.3               ether   00:e0:4c:36:00:22   C                     br1
172.16.2.15              ether   00:0c:29:bf:1f:49   C                     br1
172.16.2.6               ether   6c:3b:e5:7e:6d:68   C                     br1
172.16.1.15                      (incomplete)                              br0
10.24.8.1                ether   64:d1:54:59:37:07   C                     eth1
```

Figura 53. Tablas de enrutamiento
Fuente: Elaborada por el autor

Gestión de incidentes en la seguridad de la información: Mediante la funcionalidad de reportes e informes integrada en Endian Firewall se puede cubrir varios objetivos de control que se pueden visualizar en la Figura 54, los cuales son:

- Reporte de eventos en la seguridad de la información
- Reporte de debilidades en la seguridad
- Recolección de evidencia

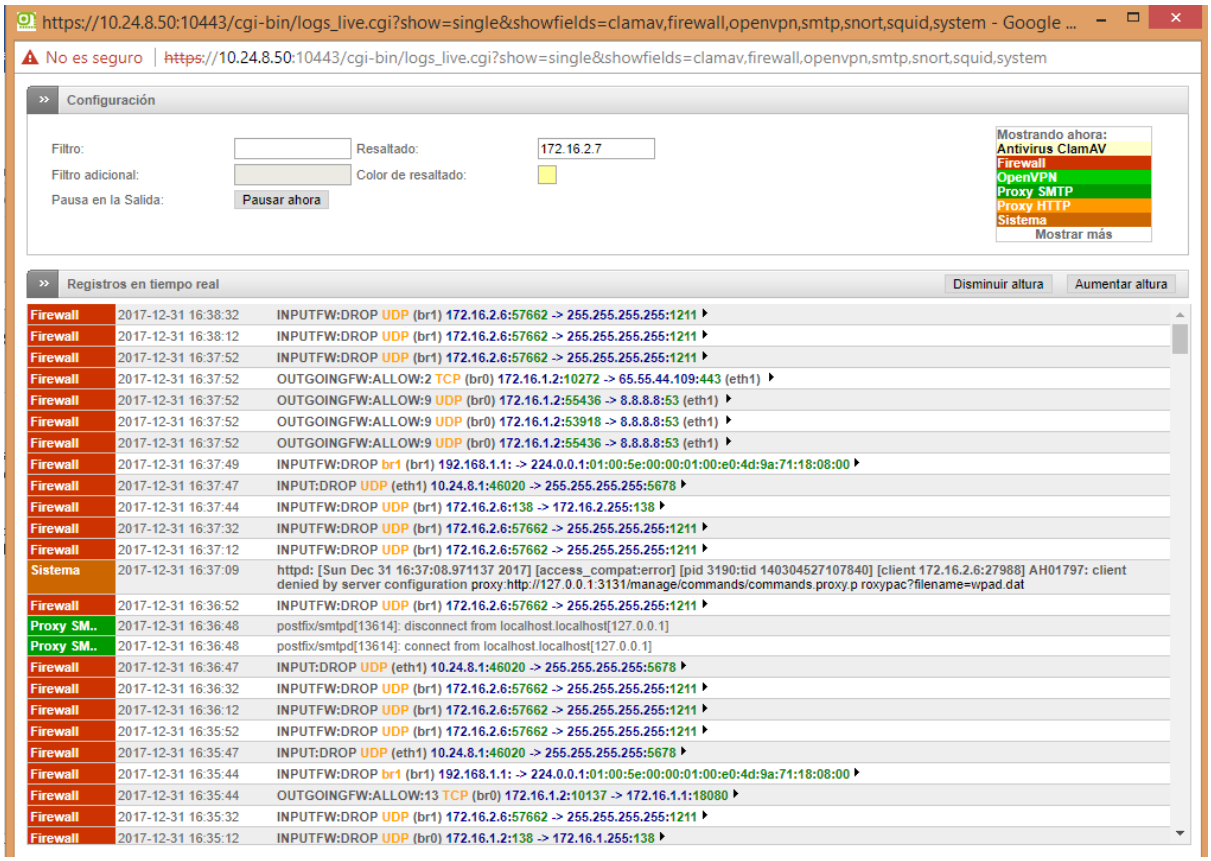


Figura 54. Sistema de reportes e informes Endian Firewall
Fuente: Elaborada por el autor

Además, la Figura 55 permite visualizar el funcionamiento de SNORT una herramienta integrada en el software Endian Firewall el cual se encarga de cumplir con el aprendizaje de los incidentes en la seguridad de la información y bloquearlos en futuros intentos de acceso.

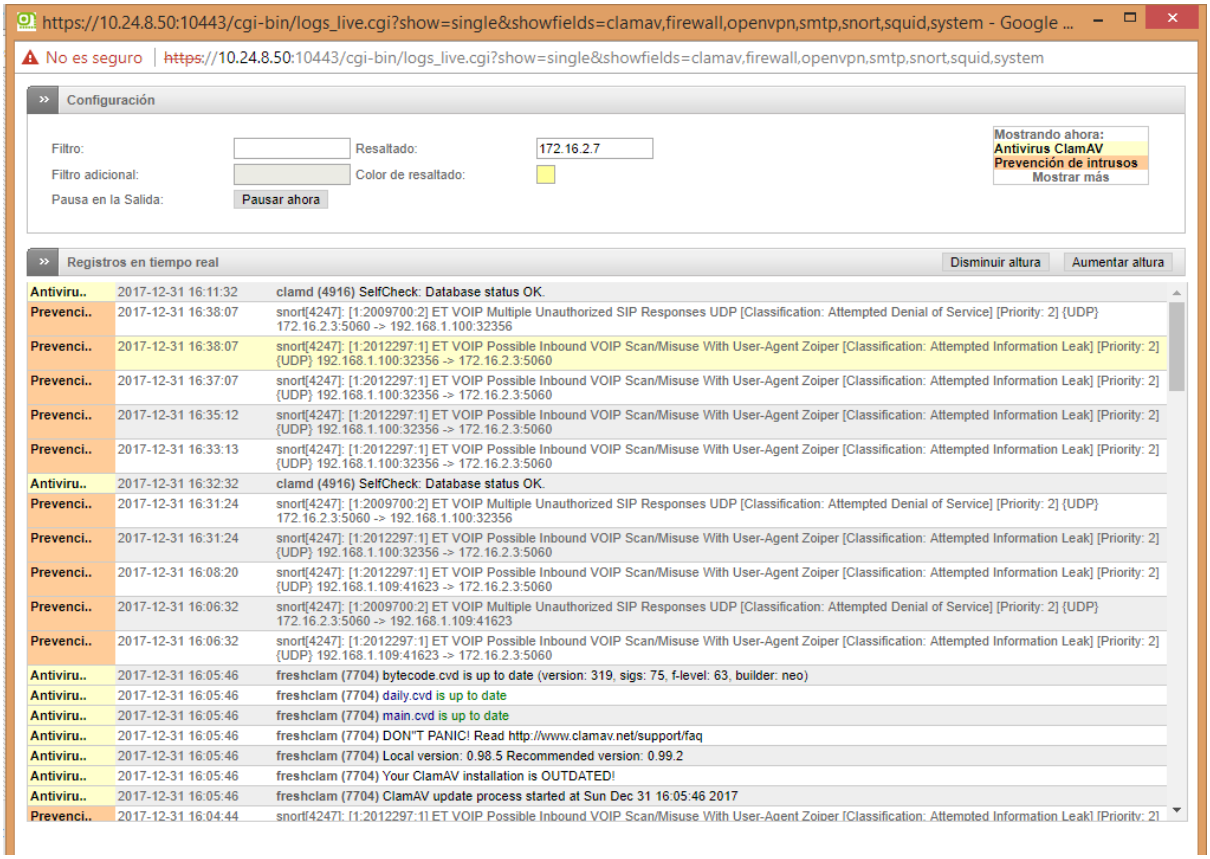


Figura 55. Visualización de alertas SNORT en Endian Firewall
Fuente: Elaborada por el autor

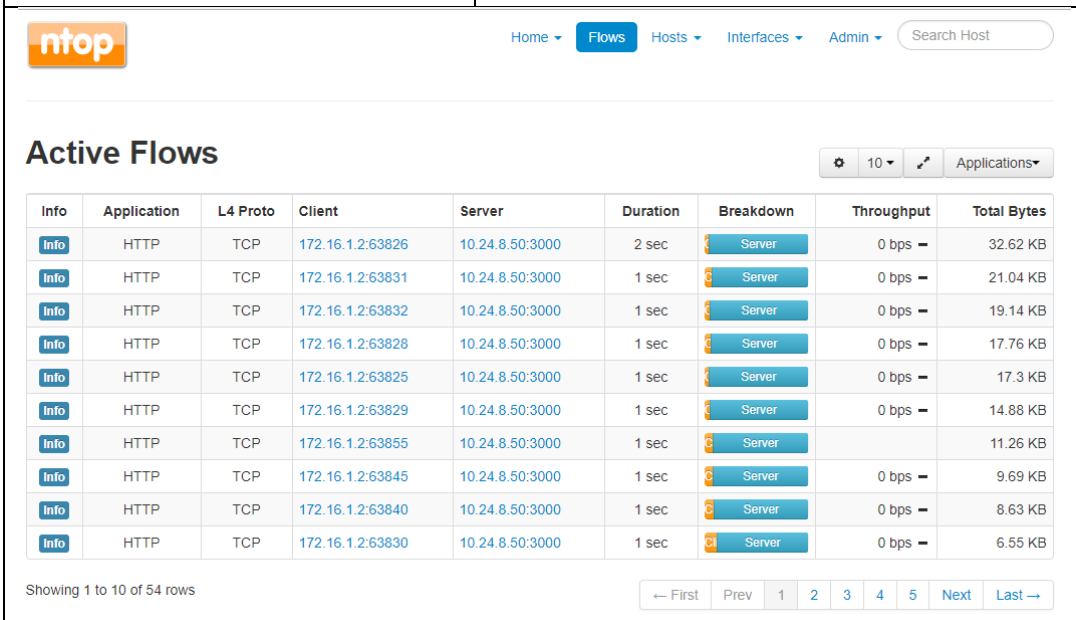
5.1. Fichas de Prueba de Funcionamiento

Se elaboro un formato de pruebas de funcionamiento que describe de manera resumida todo el proceso realizado para demostrar el funcionamiento del interfaz Endian Firewall, lo que se encuentra descrito en la Tabla 41, Tabla 42, Tabla 43, Tabla 44, Tabla 45, Tabla 46, Tabla 47, Tabla 48, Tabla 49, Tabla 50, Tabla 51, Tabla 52, Tabla 53, Tabla 54, Tabla 55, Tabla 56 y Tabla 57.

Tabla 41.
Prueba de Funcionamiento #1

Prueba de Funcionamiento	
Código	**PRF.1**
Objetivo de Control a Evaluar	Gestión de comunicación

Descripción	Probar el funcionamiento de esta herramienta se procede a observar cada uno de los interfaces que permiten monitorizar las condiciones de la red implementada
Desarrollo:	Se procede a observar en la parte de monitorización cada vez que un servidor esta activo y la interacción en la red utilizando NTOP la herramienta integrada en Endian

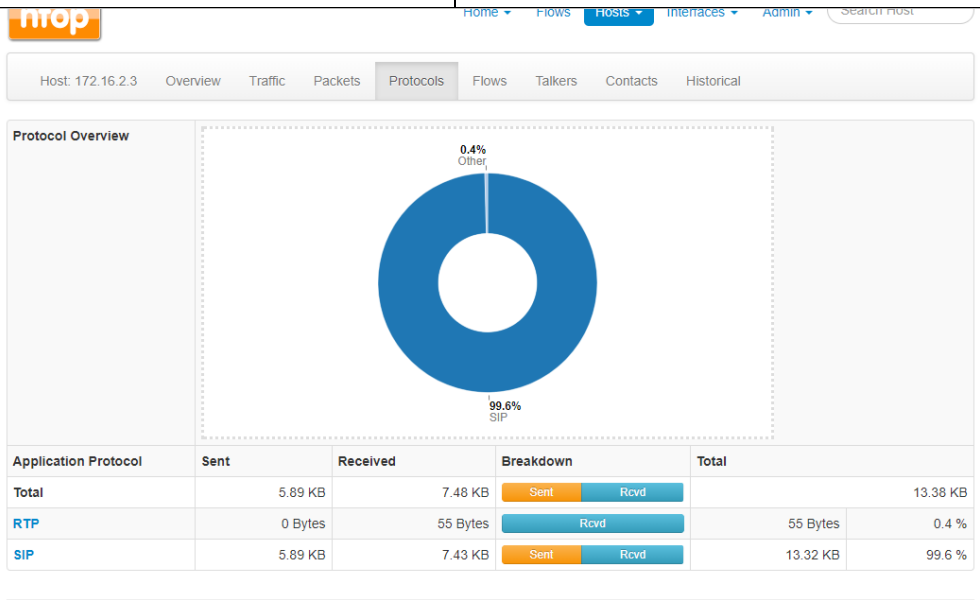


Resultado:	Se puede observar toda la información de los servidores por medio de dirección IP y el desglose de cuánto dura la conexión y el tráfico de Bytes que pasa por el mismo

Fuente: Elaborado por el autor

Tabla 42.
Prueba de Funcionamiento #2

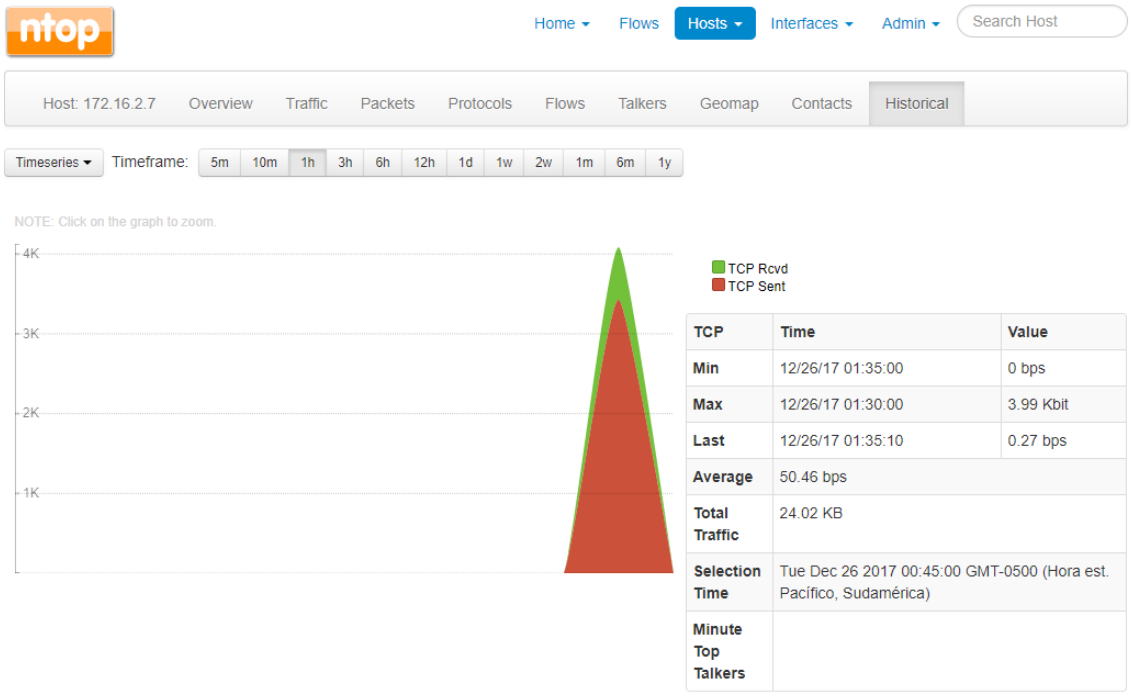
Prueba de Funcionamiento	
Código	**PRF.2**

Objetivo de Control a Evaluar	Gestión de comunicación
Descripción	Probar el funcionamiento de esta herramienta se procede a observar cada uno de los interfaces que permiten monitorizar las condiciones de la red implementada
Desarrollo:	Seleccionar un servidor dentro de la red para visualizar en tiempo real sus interacciones.
	
Resultado:	Se puede observar la información de los protocolos y el trafico de Bytes de cada protocolo que utiliza el servidor

Fuente: Elaborado por el autor

Tabla 43.
Prueba de Funcionamiento #3

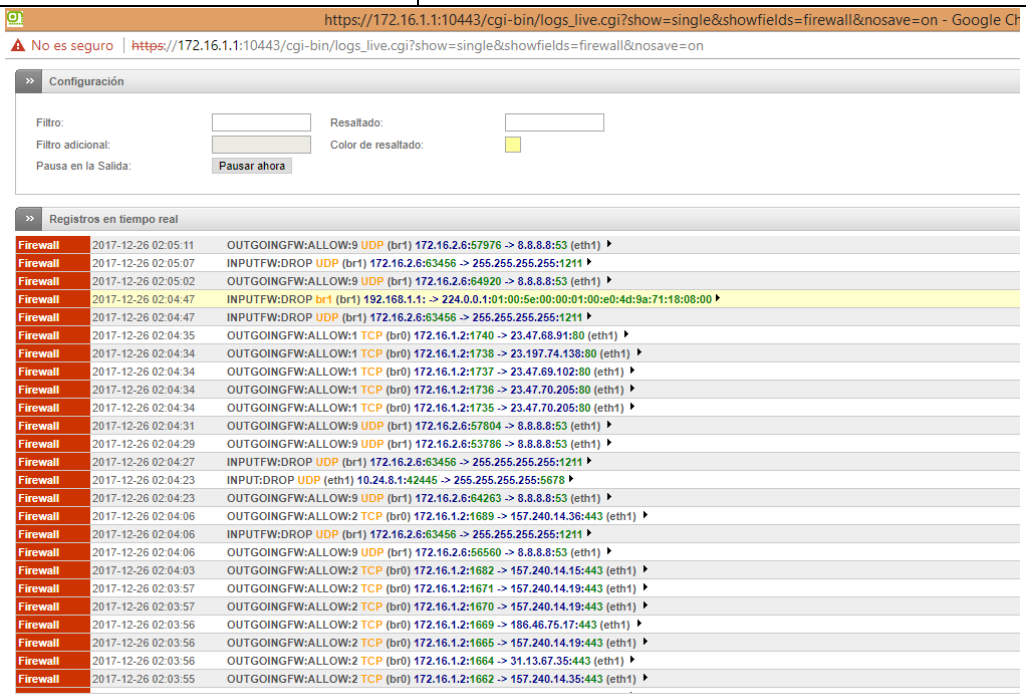
Prueba de Funcionamiento

Código	**PRF.3**
Objetivo de Control a Evaluar	Gestión de comunicación
Descripción	Probar el funcionamiento de esta herramienta se procede a observar cada uno de los interfaces que permiten monitorizar las condiciones de la red implementada
Desarrollo:	Revisión de conjunto de estadísticas diarias de la actividad del servidor y el tipo de datos que genera y recibe
	
Resultado:	Se puede observar la información del flujo de Bytes que un servidor revise de manera gráfica en base a estadísticas diarias y de tiempo real.

Fuente: Elaborado por el autor

Tabla 44.
Prueba de Funcionamiento #4

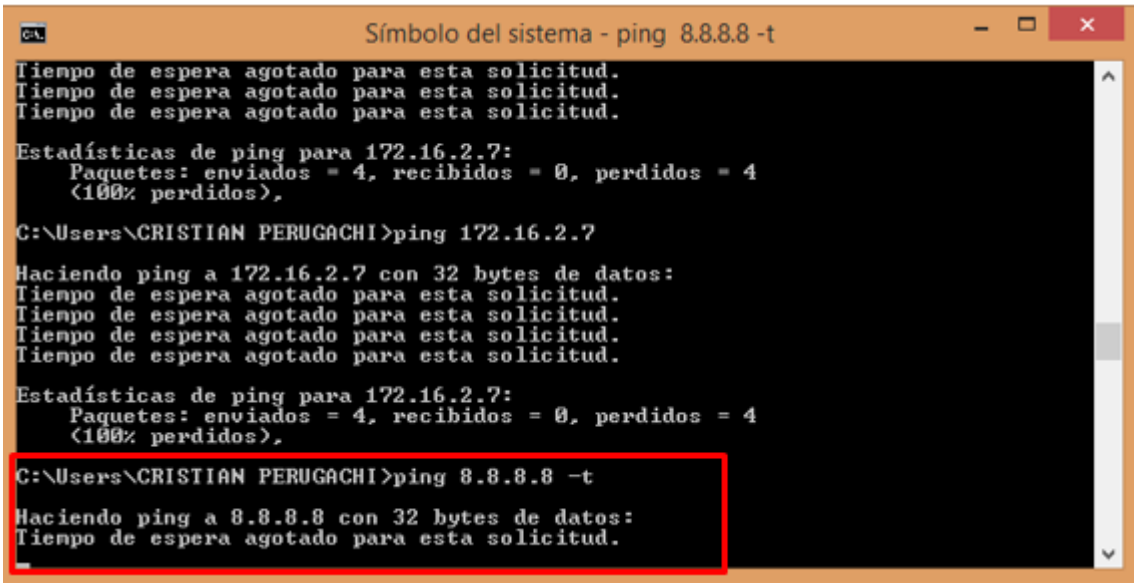
Prueba de Funcionamiento	
Código	**PRF.4**
Objetivo de Control a Evaluar	Seguridad de los servicios de red
Descripción	Endian existe la separación de redes permitiendo que la DMZ, encargada de alojar los servidores y servicios se mantenga aislada de intrusión externa no permitida, por medio de la implementación de una política de denegar todo, de esta manera solo se habilita el acceso al puerto y dirección IP específica del servicio.
Desarrollo:	Utilizar la funcionalidad de reportes para revisar en tiempo real las peticiones aceptadas o rechazadas por el firewall.



Resultado:	Se pudo observar en tiempo real los accesos permitidos y negados en el firewall en tiempo real.

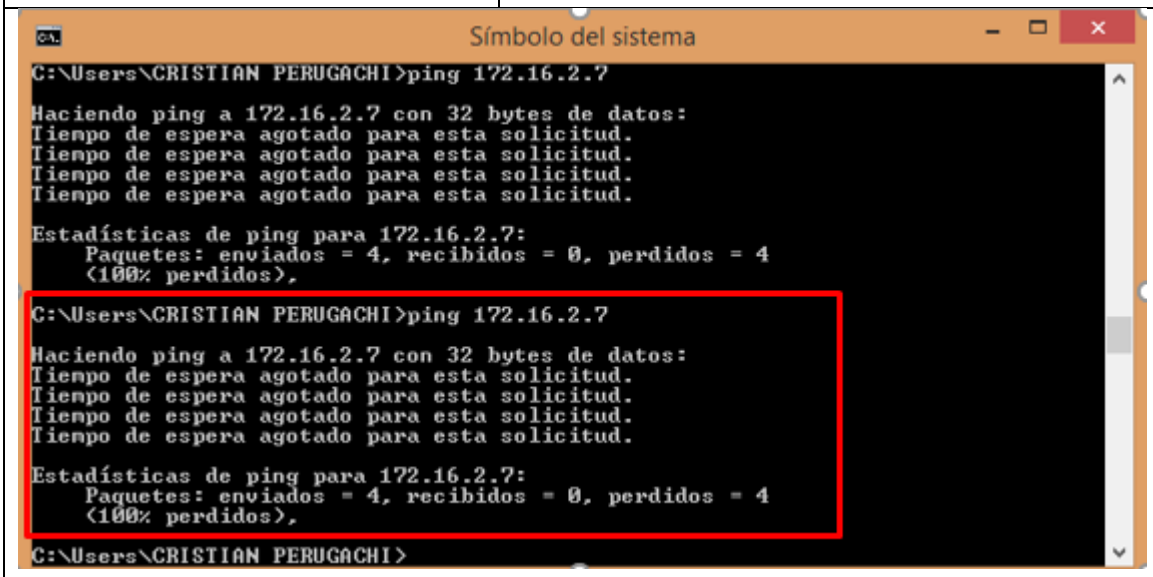
Fuente: Elaborado por el autor

Tabla 45.
Prueba de Funcionamiento #5

Prueba de Funcionamiento	
Código	**PRF.5**
Objetivo de Control a Evaluar	Seguridad de los servicios de red
Descripción	**Realización de solicitudes ICMP**
Desarrollo:	solicitud de ICMP hacia la WAN
Se 	
Resultado:	Se observa que la solicitud no se concreto debido a las reglas implementadas en el firewall

Fuente: Elaborado por el autor

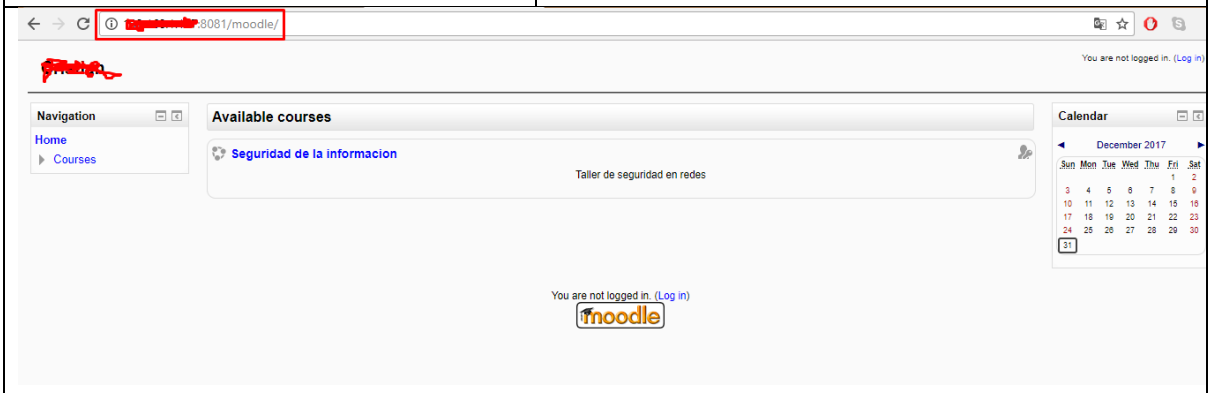
Tabla 46.
Prueba de Funcionamiento #6

Prueba de Funcionamiento	
Código	**PRF.6**
Objetivo de Control a Evaluar	Seguridad de los servicios de red
Descripción	Realización de solicitudes ICMP
Desarrollo:	Solicitud ICMP hacia la DMZ
	
Resultado:	Se observa que la solicitud no se concretó debido a las reglas implementadas en el firewall

Fuente: Elaborado por el autor

Tabla 47.
Prueba de Funcionamiento #7

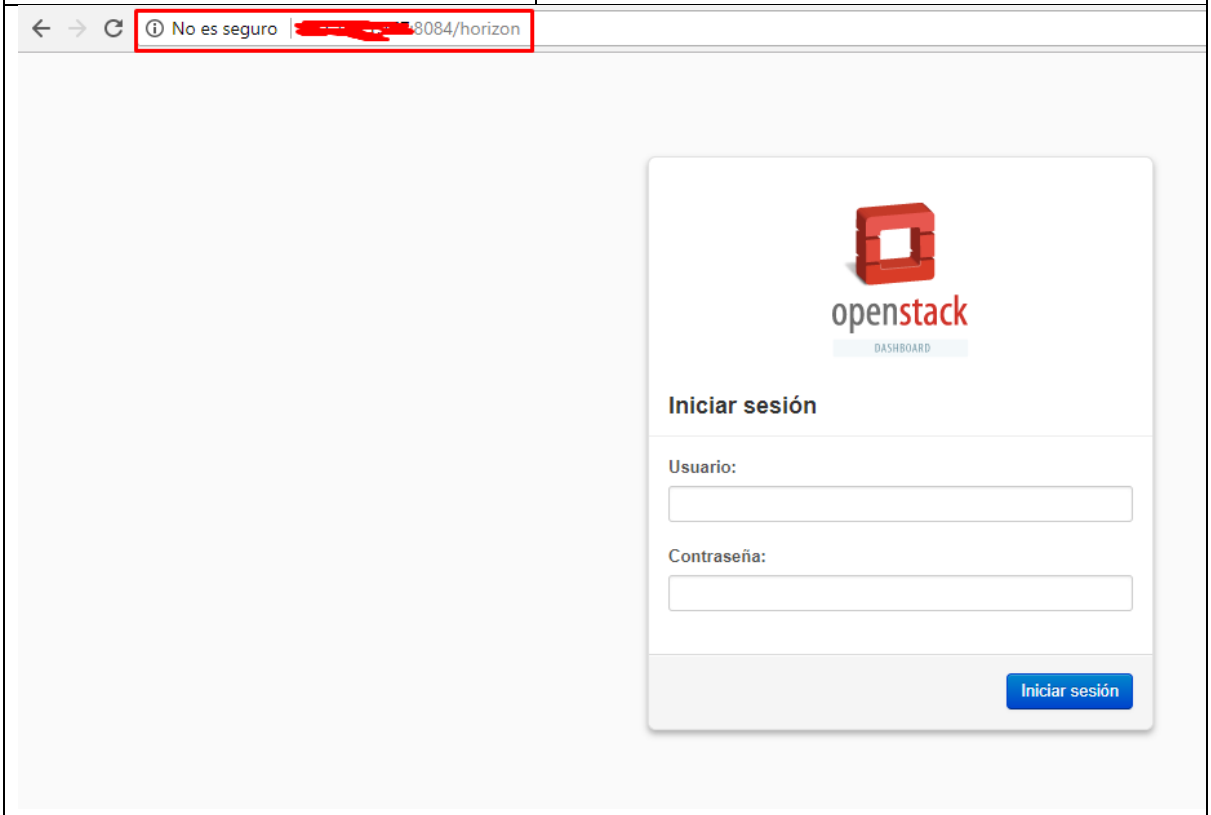
Prueba de Funcionamiento	
Código	**PRF.7**

Objetivo de Control a Evaluar	Autenticación del usuario para conexiones externas
Descripción	**Acceso por interfaz Web a servidores DMZ**
Desarrollo:	Se peticionara por medio del NAT implementado para conexiones externas apuntando al puerto asignado al servidor de moodle
	
Resultado:	Se puede observar que la regla implementada en y que se observa en la figura 35 esta operativa

Fuente: Elaborado por el autor

Tabla 48.
Prueba de Funcionamiento #8

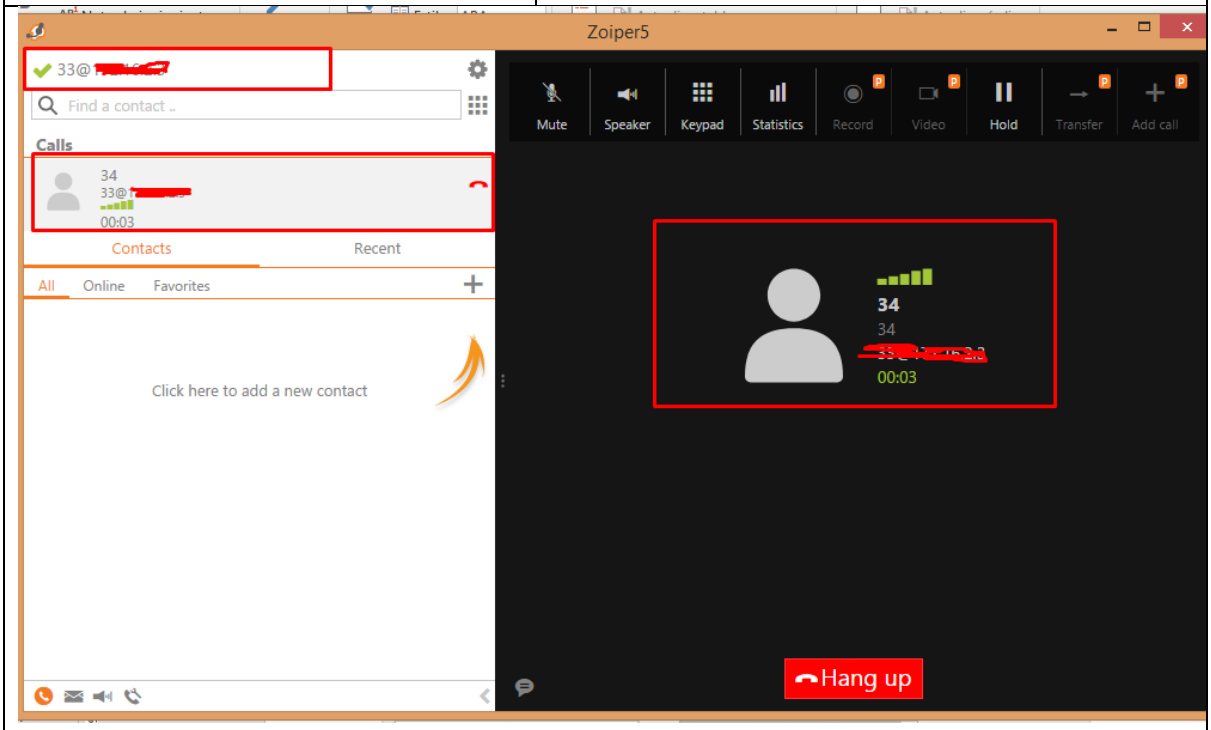
Prueba de Funcionamiento	
Código	**PRF.8**
Objetivo de Control a Evaluar	Autenticación del usuario para conexiones externas
Descripción	**Acceso por interfaz Web a servidores DMZ**

Desarrollo:	Se peticionará por medio del NAT implementado para conexiones externas apuntando al puerto asignado al servidor de openstack
	
Resultado:	Se puede observar que la regla implementada en y que se observa en la figura 35 está operativa

Fuente: Elaborado por el autor

Tabla 49.
Prueba de Funcionamiento #9

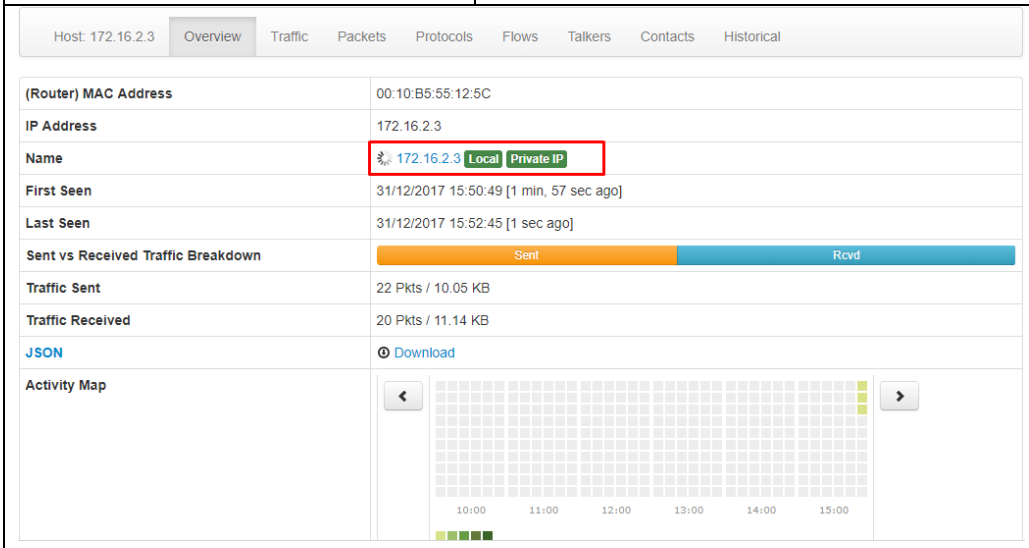
Prueba de Funcionamiento	
Código	**PRF.9**
Objetivo de Control a Evaluar	Autenticación del usuario para conexiones externas

Descripción	**Acceso por interfaz Web a servidores DMZ**
Desarrollo:	Se peticionará por medio del NAT implementado para conexiones externas apuntando al puerto asignado al servidor de voz/IP
	
Resultado:	Se puede observar que la regla implementada en y que se observa en la figura 35 está operativa

Fuente: Elaborado por el autor

Tabla 50.
Prueba de Funcionamiento #10

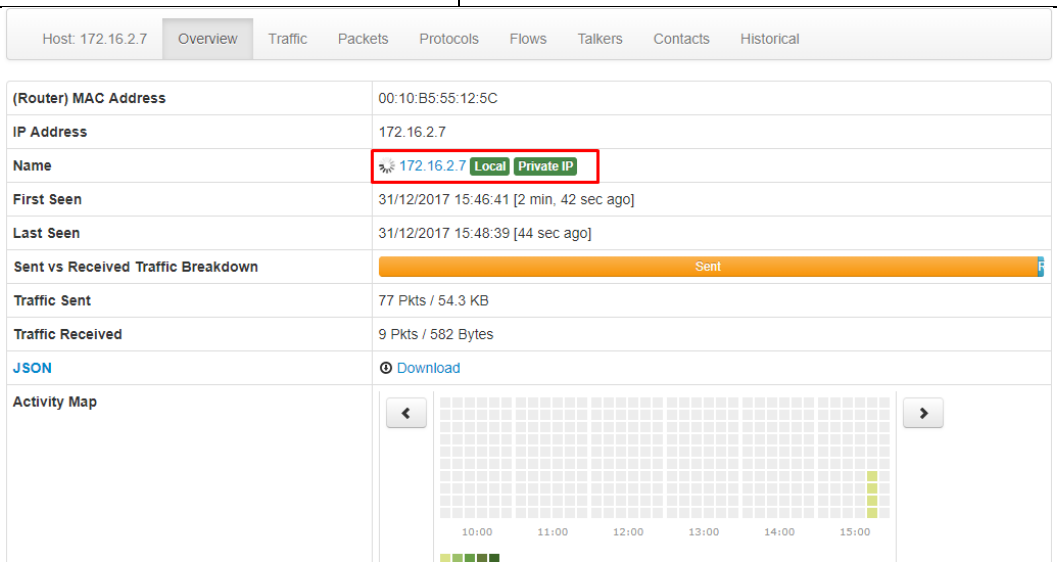
Prueba de Funcionamiento	
Código	**PRF.10**
Objetivo de Control a Evaluar	**Identificación del equipo en la red**

Descripción	visualizar los protocolos y paquetes que maneja cada uno de los servidores
Desarrollo:	Se utilizara la herramienta NTOP para verificar el flujo de datos que maneja el servidor Voz/IP
	
Resultado:	Se puede observar el flujo de datos que peticiona el servidor

Fuente: Elaborado por el autor

Tabla 51.
Prueba de Funcionamiento #11

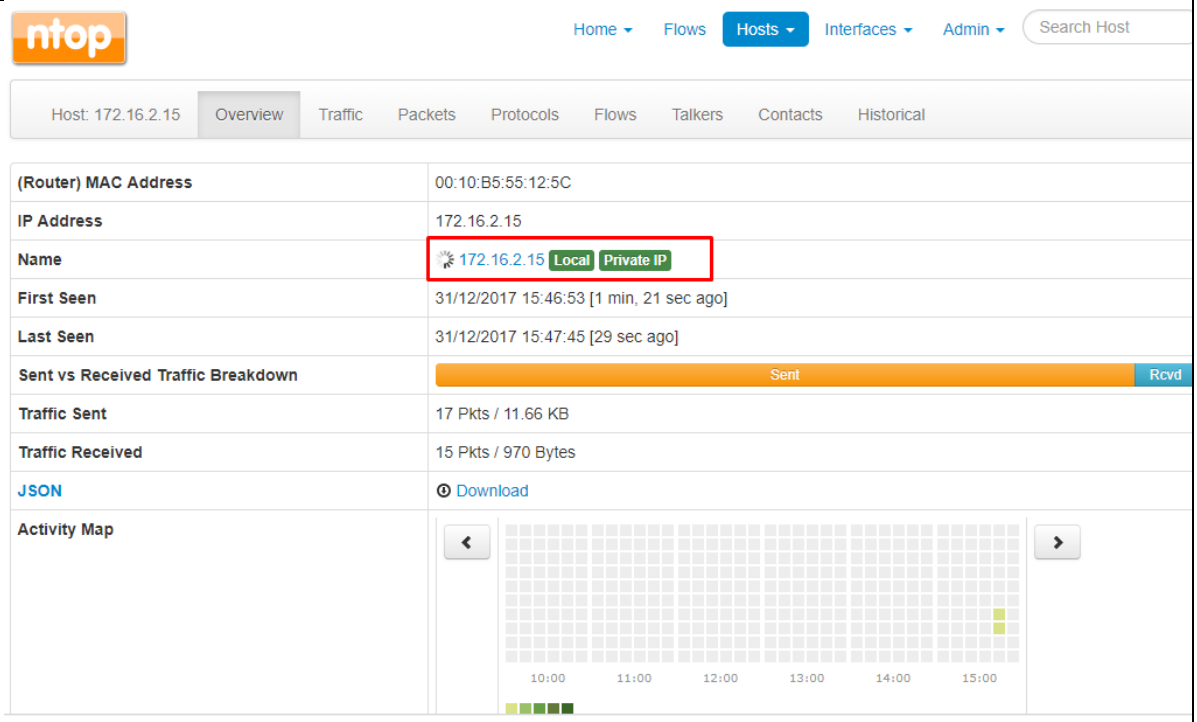
Prueba de Funcionamiento	
Código	**PRF.11**
Objetivo de Control a Evaluar	**Identificación del equipo en la red**
Descripción	visualizar los protocolos y paquetes que maneja cada uno de los servidores

Desarrollo:	Se utilizara la herramienta NTOP para verificar el flujo de datos que maneja el servidor moodle
	
Resultado:	Se puede observar el flujo de datos que peticiona el servidor

Fuente: Elaborado por el autor

Tabla 52.
Prueba de Funcionamiento #12

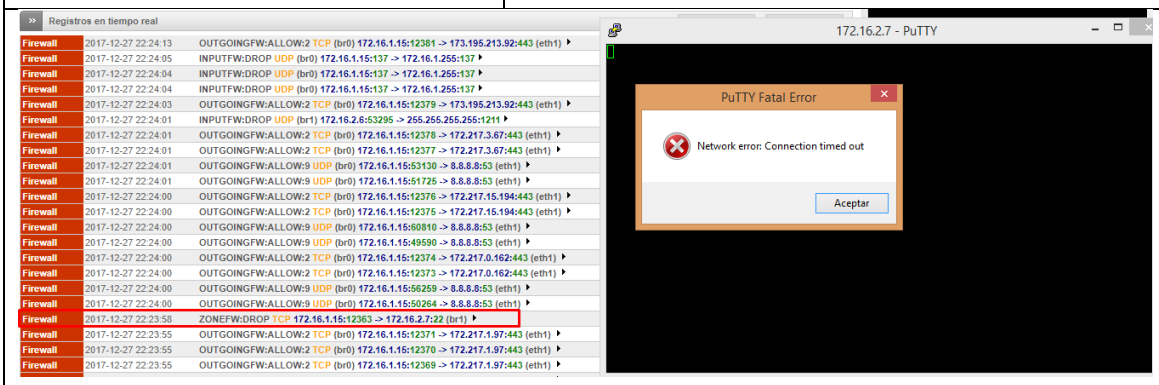
Prueba de Funcionamiento	
Código	**PRF.12**
Objetivo de Control a Evaluar	**Identificación del equipo en la red**
Descripción	visualizar los protocolos y paquetes que maneja cada uno de los servidores

Desarrollo:	Se utilizará la herramienta NTOP para verificar el flujo de datos que maneja el servidor openstack
	
Resultado:	Se puede observar el flujo de datos que peticiona el servidor

Fuente: Elaborado por el autor

Tabla 53.
Prueba de Funcionamiento #13

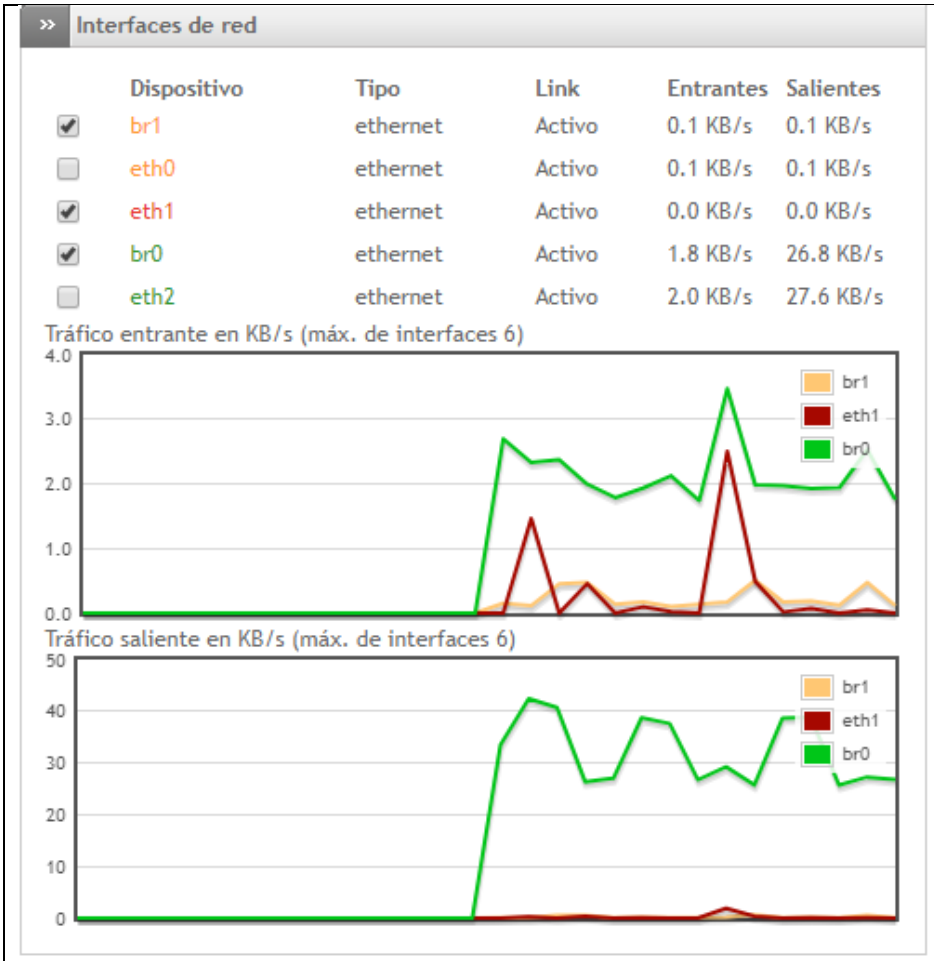
Prueba de Funcionamiento	
Código	**PRF.13**
Objetivo de Control a Evaluar	Protección del puerto de diagnóstico remoto
Descripción	Reglas de acceso SSH para los servidores por medio de IP de administrador

Desarrollo:	Se implemento una regla de acceso para el puerto remoto SSH que permita acceso solo por medio de una IP de administrador. Si se utiliza una ip no permitida.
	
Resultado:	Se puede observar que el firewall deniega el acceso a la IP no permitida para acceso remoto.

Fuente: Elaborado por el autor

Tabla 54.
Prueba de Funcionamiento #14

Prueba de Funcionamiento	
Código	**PRF.14**
Objetivo de Control a Evaluar	**Segregación de redes**
Descripción	Endian Firewall separa las redes en LAN, DMZ y WAN con sus respectivos colores verde, naranja y rojo.
Desarrollo:	Se verifica mediante el interfaz grafico que las redes estén activas y la interacción que realizan.

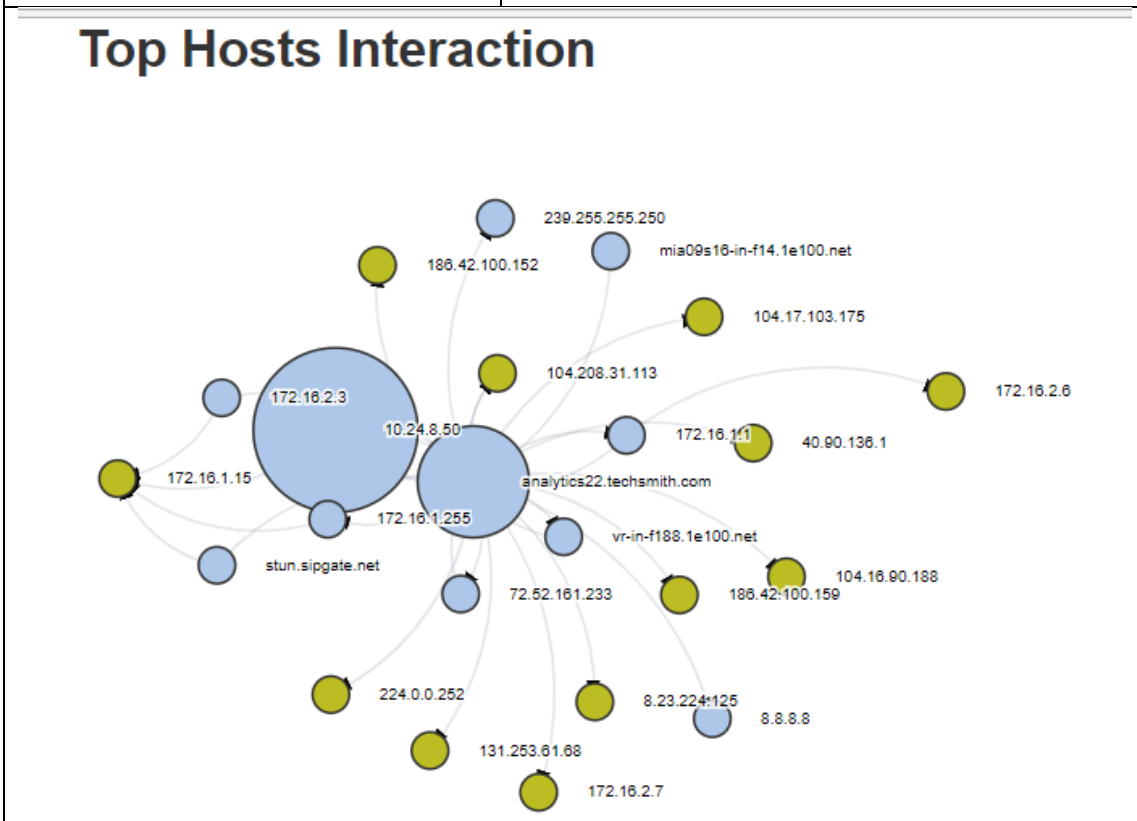


Resultado:	Se puede observar en tiempo real el flujo de datos que maneja cada interfaz tanto saliente como entrante.

Fuente: Elaborado por el autor

Tabla 55.
Prueba de Funcionamiento #15

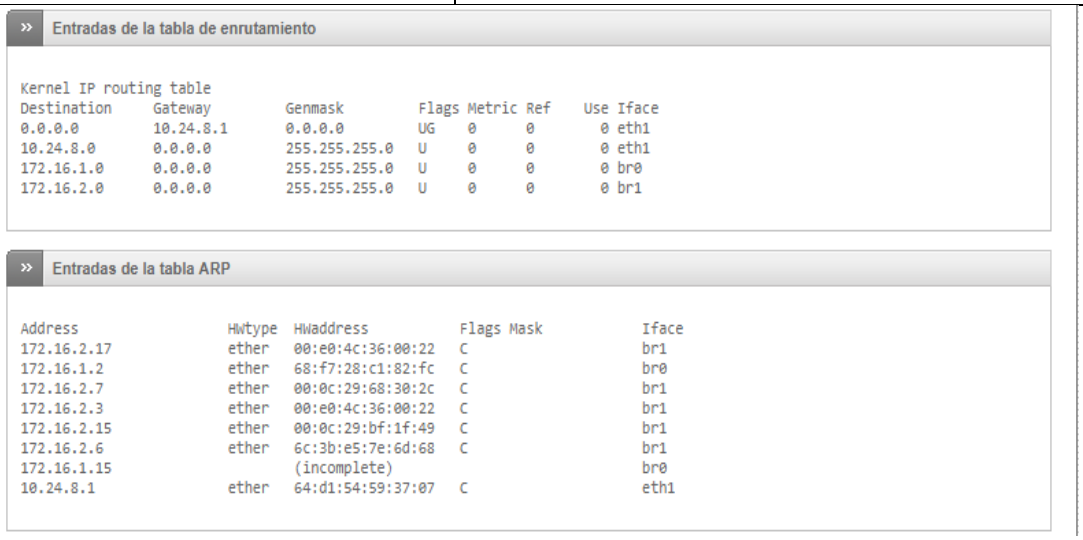
Prueba de Funcionamiento	
Código	**PRF.15**
Objetivo de Control a Evaluar	**Control de conexión**
Descripción	Se visualiza todas las interacciones y conexiones a través de Endian Firewall

Desarrollo:	Se utiliza la herramienta NTOP para visualizar el diagrama de interacciones lógicas de la red.
	
Resultado:	Se puede observar en tiempo real todas las interacciones de los servidores y host en la red.

Fuente: Elaborado por el autor

Tabla 56. Prueba de Funcionamiento #16
Prueba de Funcionamiento #16

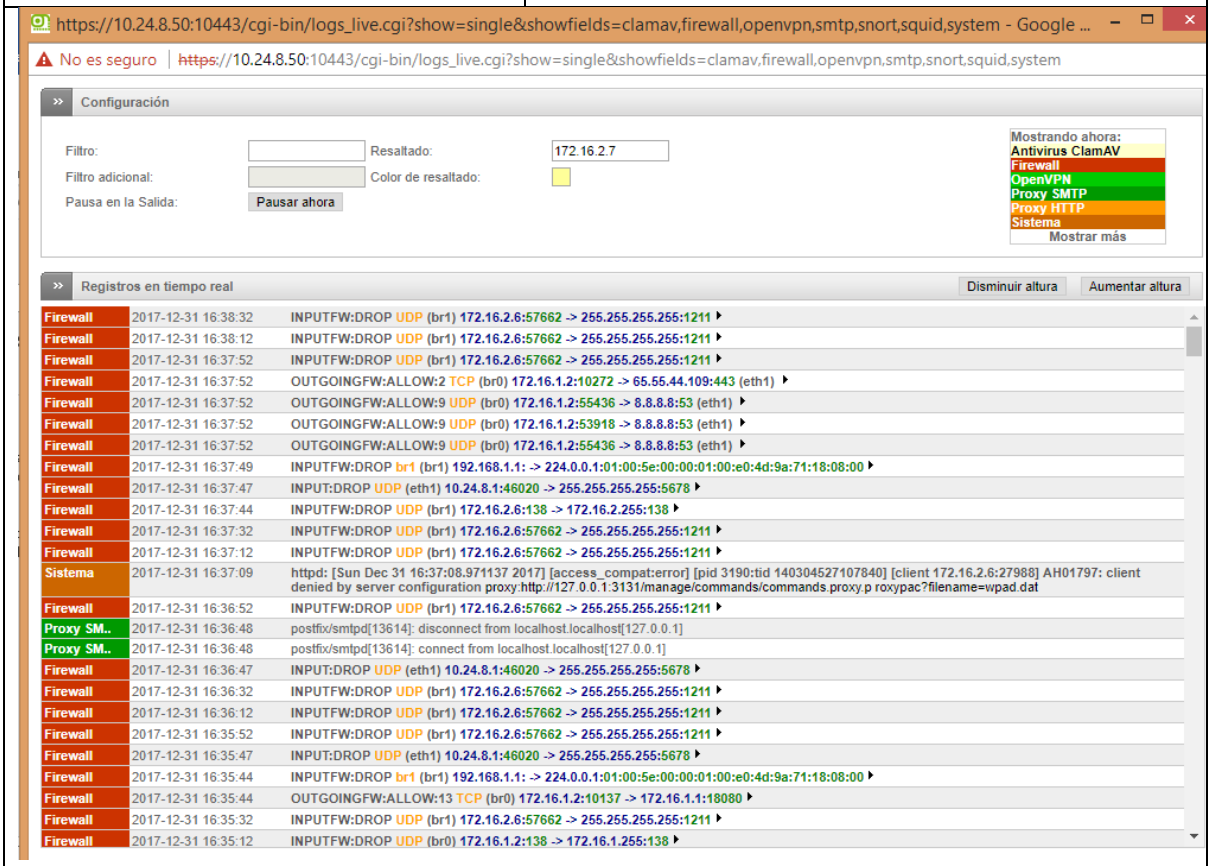
Prueba de Funcionamiento	
Código	**PRF.16**
Objetivo de Control a Evaluar	**Control de routing de redes**
Descripción	Visualizar todas las rutas de routing implementadas

Desarrollo:	Mediante el interfaz grafico de Endian Firewall se procede a visualizar la tabla de enrutamiento.
	
Resultado:	Se puede observar la tabla de enrutamiento y la tabla ARP.

Fuente: Elaborado por el autor

Tabla 57.
Prueba de Funcionamiento #17

Prueba de Funcionamiento	
Código	**PRF.17**
Objetivo de Control a Evaluar	**Gestión de incidentes en la seguridad de la información**
Descripción	Visualizar los reportes de cada herramienta integrada en endian Firewall

Desarrollo:	Utilizar el interfaz web de Endian firewall para visualizar los reportes de las herramientas implementadas.
	
Resultado:	Se puede observar las herramientas implementadas y su reporte en tiempo real de la interacción que procede con la red.

Fuente: Elaborado por el autor

Una vez realizadas todas las pruebas de funcionamiento se procede a elaborar un resumen de todas las pruebas elaboradas conglomerado en la Tabla 58. En donde se puede observar que pruebas se realizaron y que resultado se obtuvo.

Tabla 58.
Resumen pruebas de funcionamiento

Pruebas de Funcionamiento		
Código	**Correcto**	**Incorrecto**
PRF.1	X	
PRF.2	X	
PRF.3	X	
PRF.4	X	
PRF.5	X	
PRF.6	X	
PRF.7	X	
PRF.8	X	
PRF.9	X	
PRF.10	X	
PRF.11	X	
PRF.12	X	
PRF.13	X	
PRF.14	X	
PRF.15	X	
PRF.16	X	
PRF.17	X	

Fuente: Elaborado por el autor

En la tabla 58 se puede observar que todos los objetivos de control implementados se pueden verificar con la funcionalidad de las herramientas y las pruebas de funcionamiento realizado.

Análisis de riesgo

En base a las políticas y objetivos de control implementados se procede a la revaloración de las amenazas restando en base a MAGERIT las amenazas se disminuyen si existen salvaguardas, el desglosado de la nueva valoración se encuentra realizada en Excel y capturada con su respectivo calculo en el Anexo 19.

De este análisis con la misma herramienta se obtiene un promedio de resultados en Excel que nos presenta el riesgo potencial después de implementar las políticas y salvaguardas por medio del software detallado en la Tabla 59.

Además se utilizó una herramienta que se llama GFI Languar que es un escáner de vulnerabilidades que realiza más 10000 pruebas de seguridad informática y expresa en una

escala de Bajo, Medio y Alto el riesgo potencial al que esta expuesta la organización y los resultados son similares a los obtenidos por medio de la aplicación de la metodología de valoración que se encuentra en el Libro II de MAGERIT, estos resultados se encuentran en el Anexo 20.

Tabla 59.
Riesgo Potencial con políticas y salvaguardas implementadas

		Probabilidad de Amenaza			
		Origen Natural	Origen Industrial	Origen Humano (Accidental)	Origen Humano (Deliberado)
Magnitud del Daño	Data-Center	5,6	5,6	4,6	4,1

Fuente: Elaborada por el autor

De lo que se puede observar que el riesgo por origen humano tanto accidental como deliberado disminuye 4,6 y 4,1 lo que implica un nivel bajo que es aceptable para una organización según el Libro I de MAGERIT.

5.2. Estudio Económico

Para definir el costo directo de cada proceso es necesario repasar las etapas del proyecto, las cuales son:

- Auditoria y Diseño
- Implementación y Pruebas de Funcionamiento

Auditoria y Diseño: Para este proceso utilizo un tiempo promedio de 128 horas que se dividieron en el transcurso de dos meses, cada una de las actividades contaron con la utilización de materiales y cada costo esta detallado en la Tabla 60. Los precios expuestos se ajustan al mercado actual.

“Lo primero –señala Daniel Suárez, director de Contigo– es ponerte un sueldo. ¿Cuánto vas a ganar? Por ejemplo, 2.000 euros al mes. A ese sueldo, le sumas la parte correspondiente de

Seguridad Social, gasolina, renting del coche, la oficina… y todos aquellos costes que quieras imputar. Ya tienes 4.000 euros de gastos al mes" (Escudero, 2017)

Lo que implica que en base a valores del mercado se considera que un empleado público de noveno nivel percibe 2034 dólares mensuales más un total de 1000 en gastos adicionales suma un total de 3034 dividido para las 160 horas al mes, resulta en un total de 18,96 dólares por hora.

Tabla 60.
Costo Directo Auditoria Data-Center

		UNIDAD DE MEDIDA	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
COSTOS DIRECTOS	**TALENTO HUMANO**	Horas	auditor de redes de datos	128	$ 18,96	$ 2.426,00
		Total				$ 2.426,00
	ÚTILES DE OFICINA	Unidades	hojas	200	$ 0,01	$ 2,00
		Unidades	Esferos	5	$ 0,50	$ 2,50
		Unidades	Carpetas	2	$ 1,00	$ 2,00
		Unidades	cuadernos	2	$ 1,00	$ 2,00
		Unidades	varios	1	$ 10,00	$ 10,00
		Total				$ 18,50
	DEPRECIACIONES					
	EQUIPO DE COMPUTACIÓN	meses	Lenovo core I7	1	$ 400,0	$ 400,00
		Total				$ 400,00
Total						$ 2.45,38

Fuente: Elaborada por el autor

Implementación y pruebas de funcionamiento: Para esta etapa del proceso se utilizó un total de 32 horas que se dividieron en un periodo de dos semanas, los costos directos se pueden observar en la Tabla 61.

Tabla 61.
Costo Directo Implementación y Pruebas de funcionamiento Firewall

		UNIDAD DE MEDIDA	DESCRIPCIÓN	CANTIDAD	VALOR UNITRIO	VALOR TOTAL
COSTOS DIRECTOS	**TALENTO HUMANO**	Horas	Ingeniero en electrónica y redes	32	$ 18,96	$ 606,72
		Total				$ 606,72

	MATERIALES	Unidades	HP Proliant DL 150 G9	1	$ 1.987,00	$ 1.987,00
		Unidades	Tarjeta de Red Gigabit HP	1	$ 150,00	$ 150,00
		Unidades	Licencia Endian Firewall	1	$ 588,00	$ 588,00
		Total				$ 2.725,00
	EQUIPO DE COMPUTACIÓN	**DEPRECIACIONES**				
		meses	Lenovo core I7	1	$ 400,00	$ 400,00
		Total				$ 400,00
	Total					$ 3.731,72

Fuente: Elaborada por el autor

5.3. Costo/Beneficio

El costo de implementación de un firewall dedicado con todas las licencias de funcionamiento en base a varias cotizaciones obtenidas de un servidor dedicado en la página OVH que brinda servicios donde se genera un costo de instalación del equipo de 1290 USD y un costo aproximado de 325 USD por mes lo que implicaría un gasto de 3900 USD anual en caso de arrendamiento para un cisco ASA, mientras que comprar un cisco ASA tiene un costo de 1800 USD. El ahorro al contar con un equipo físico disponible para instalar el software Endian Firewall que cumple con los objetivos de control planteados es de 1800 USD. (OVH, 2017).

El beneficio que obtiene la facultad con la implementación de Endian Firewall es el siguiente:

- Segregación de redes para mejorar la interacción de los usuarios finales con los servidores a los que se envía a la DMZ con una política de denegar todo.
- Control de acceso mediante un sistema de firewall basado en debian, además de un servidor vpn que permite realizar accesos remotos punto a punto de forma segura. También es posible controlar tiempos de acceso en base a su herramienta squid implementada y control de acceso radius mediante su autenticador integrado.

- Sistema de monitorización basado en NTOP que permite ver los paquetes que transitan por la red y elaborar diagrama de interacción entre host y servidores, además permite revisar el ancho de banda de cada interfaz y todo lo antes mencionado en tiempo real con un interfaz amigable con el administrador
- Protección de la información en cada uno de los servidores mediante cada una de las herramientas integradas en el software que permiten autoaprendizaje y prevención de intrusos.
- Sistema de reportes de incidentes diarios que permiten evaluar las condiciones de la infraestructura.
- Bloqueo de páginas mediante un proceso de listas negras, a su vez también permite bloqueo de correo con cadenas reconocidas como spam o por inserción en la lista negra de correos para su rechazo automático.

Además de los beneficios que presenta el establecimiento de políticas y procedimientos es el siguiente:

- Mejorar los tiempos de respuesta ante amenazas por medio de procesos claros en caso de presentarse cualquier amenaza.
- Mantener una constante documentación de los incidentes que afecten la infraestructura
- Planificación periódica de mejoras en la infraestructura y sus controles para prevenir futuras amenazas.

Conclusiones

- La norma ISO/IEC 27001 permite adaptar sus objetivos de control a la organización conformada por los activos que integran el Data-Center de la Facultad de ingeniería y ciencias aplicadas en lo que respecta a los objetivos de control referente a la seguridad de la información y a su vez mediante los procesos para la elaboración de un manual de políticas que regula la parte administrativa del personal a cargo de los servidores y equipos que procesan los datos y los servidores.
- Con la estandarización de los procesos en el Data-Center por medio de los manuales de políticas, manuales de procedimientos y los formatos para la elaboración de los procesos se reduce los tiempos de respuesta ante amenazas en la seguridad de la información, además de permitir una documentación de cada actividad realizada, reducir las amenazas de origen humado accidental y deliberado las cuales se encontraban inicialmente en parámetros de 8,6 y 9,3 respectivamente indicando un riesgo potencial medio, y al finalizar la implementación se redujeron a 4,6 y 4,1 indicando nivel bajo.
- La facultad de ingeniería y ciencias aplicadas mantiene una infraestructura interna de servidores y equipos de procesamiento de información con crecimiento y desarrollo constante, al tratarse de una organización publica para el análisis de riesgos inicial se utilizó MAGERIT que es un método desarrollado por el gobierno español que permite de una manera estructurada identificar las condiciones del Data-Center.
- Seleccionar MAGERIT como el método para analizar los riesgos permitió simplificar el proceso de identificar los activos que posee el Data-Center, su clasificación, la importancia para la organización, las amenazas a las que se

expone y también si existen salvaguardas que protejan cada elemento y proceso; a su vez permite elaborar mediante un método de cálculo de tablas las condiciones iniciales de la infraestructura.

- Debido a las condiciones de la organización tanto en materia de infraestructura lógica como en estructura organizacional los objetivos de control seleccionados permiten mejorar las características iniciales del Data-Center, además de permitir una constante evolución y mejora continua de las herramientas y procesos seleccionados.
- Endian Firewall es la herramienta de código abierto que actualmente permite cumplir con la mayoría de objetivos de control presentados en el diseño de la metodología de gestión de seguridad de la información, además permite utilizar sus herramientas de manera libre y solo se ve limitado por las características físicas del equipo seleccionado para su implementación.
- No existen sistemas de seguridad de la información perfectos, porque los equipos de procesamiento de datos, así como los equipos donde se implementan los servidores dependen de condiciones tanto físicas como lógicas, por lo que cualquier proceso implementado debe estar en constante evaluación, planificación y desarrollo para reducir los riesgos de ataques o vulnerabilidades que se puedan presentar por evolución de la tecnología.

Recomendaciones

- Para optimizar los procesos es recomendable modificar la estructura organizacional actual que presenta un modelo descentralizado, por un sistema centralizado con departamentos técnicos que se encarguen de los procesos establecidos en la normativa de manera independiente.
- Es recomendable generar un proceso de inducción para todas las personas que conforman el Data-Center en donde se informe acerca de las políticas existentes y los procesos establecidos.
- Para la implementación de cualquier servidor o equipo de red en la infraestructura y topología tanto física como lógica del Data-Center, es mejor realizarla en horarios no laborales o de baja ocupación de los servicios integrados para no afectar el funcionamiento de las prestaciones de la red.
- Al momento de implementar un nuevo servicio o equipo de comunicación es importante ser lo menos intrusivo posible y evitar afectar la disponibilidad de los sistemas de información, además se sugiere para implementaciones utilizar horarios no laborales.
- Se recomendable utilizar la red inalámbrica mediante un enlace hacia el firewall implementado que permita generar un entorno de pruebas para los servidores implementados y la interacción con los estudiantes, docentes y administrativos que conforman la Facultad de ingeniería y ciencias aplicadas.
- En caso de realizar pruebas de funcionamiento, mantenimiento o instalación de nuevos equipos, se recomienda identificar el área de trabajo para de esta manera aislar el entorno y afectar en menor medida las prestaciones que la infraestructura ofrece a los usuarios finales.

- Es recomendable realizar una planificación constante trimestral donde se evalué los informes del sistema implementado y de las salvaguardas existentes para proponer soluciones de mejora en caso de ser necesario.

Anexos

Anexo 1: Objetivos De Control Y Controles De La Norma ISO 27001 Orientados A La Seguridad Lógica De La Red

A.5 Políticas de seguridad de la información		
A.5.1 Directrices de la dirección en la seguridad de la información		
Objetivo: Proporciona las directrices de la dirección y el soporte para la información de la seguridad en acuerdo con los requerimientos del negocio en base a las leyes y regulaciones		
A.5.1.1	Políticas para la seguridad de la información	Control Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.
A.5.1.2	Revisión de las políticas de la seguridad de la información	Control Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad
A.6 Organización de seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.		
A.6.1.1	Asignación de responsabilidades para la SI	Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.
A.6.1.2	Segregación de tareas	Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización
A.6.1.3	Contacto con las autoridades	Deben ser establecidos los contactos apropiados con las autoridades.
A.6.1.4	Contacto con grupos de interés especial	Mantener contacto con grupos de interés especial en

		seguridad y asociaciones profesionales.
A.6.1.5	Seguridad de la información para la gestión de proyectos	La seguridad de la información debe ser direccionada en la gestión de proyectos, dependiendo del tipo de proyecto
A.6.2 Dispositivos móviles y tele-trabajo		
Objetivo: Asegurar la seguridad en el tele-trabajo y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Una política que permita dar soporte para las fallas en la seguridad generadas por adoptar el uso de dispositivos móviles
A.6.2.2	Tele-trabajo	Una política debe ser implementada para proteger la informacion de acceso, procesamiento y almacenamiento en tele-trabajo
A.7 Seguridad en recursos humanos		
A.7.1 Antes de la contratación		
Objetivo: Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.		
A.7.1.1	Investigación de antecedentes	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.7.1.2	Términos y condiciones de contratación	Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.
A.7.2 Durante la contratación		
Objetivo: Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.		

A.7.2.1	Responsabilidades de gestión	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.
A.7.2.2	Concienciación, educación y capacitación en SI	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
A.7.2.3	Proceso disciplinario	Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.
A.8 Gestión de Activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.		
A.8.1.1	Inventario de activos	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
A.8.1.2	Propiedad de los activos	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.8.1.3	Uso aceptable de los activos	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que

		estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.
A.8.2 Clasificación de la información		
Objetivos: Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.		
A.8.2.1	Directrices de clasificación	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.
A.8.2.2	Etiquetado y manipulado de la información	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.2.3	Manipulación de activos	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
A.8.3 Manejo de medios de almacenamiento		
Objetivo: Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.		
A.8.3.1	Gestión de soportes extraíbles	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o

		corrupción durante el transporte fuera de los límites físicos de la organización.
A.9 Control de Acceso		
A.9.1 Requisitos de negocio para el control de Accesos		
Objetivo: Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.		
A.9.1.1	Política de control de accesos:	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
A.9.1.2	Control de acceso a las redes y servicios asociados	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
A.9.2 Gestión de Acceso de Usuario		
Objetivo: Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.		
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

A.9.2.6	Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
A.9.3 Responsabilidades de usuario		
Objetivo: Asegurar las cuentas de usuarios para proteger su información de autenticación.		
A.9.3.1	Uso de información confidencial para la autenticación	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
A.9.4 Control de acceso para sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a las aplicaciones y sistemas		
A.9.4.1	Restricción del acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on
A.9.4.3	Gestión de contraseñas de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.
A.9.4.4	Uso de herramientas de administración de sistemas	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.
A.9.4.5	Control de acceso al código fuente de los programas	Se debería restringir el acceso al código fuente de las aplicaciones software.
A.10 Cifrado		
A.10.1 Controles de cifrado		
Objetivo: Prevenir un uso efectivo de cifrado para asegurar la confidencialidad, disponibilidad e integridad de la información.		

A.10.1.1	Política de uso de los controles criptográficos	Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de claves	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.
A.11 Seguridad física y ambiental		
A.11.1 Áreas Seguras		
Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.		
A.11.1	Perímetro de seguridad física	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.
A.11.2	Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.
A.11.3	Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
A.11.4	Protección contra las amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.5	El trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.
A.11.6	Áreas de acceso público, carga y descarga	Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones

		de procesamiento de información.
A.11.2 Equipos		
Objetivo: Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.		
A.11.2.1	Emplazamiento y protección de equipos	Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
A.11.2.2	Instalaciones de suministro	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.
A.11.2.3	Seguridad del cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.
A.11.2.4	Mantenimiento de los equipos	Los equipos deberían mantenerse de forma correcta con el objeto de garantizar su disponibilidad e integridad continuas.
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura

		antes de su eliminación o reutilización.
A.11.2.8	Equipo informático de usuario desatendido	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.
A.12 Seguridades Operativas		
A.12.1 Responsabilidades y Seguridad operacional		
Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados.		
A.12.1.1	Documentación de procedimientos de operación	Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
A.12.1.3	Gestión de capacidades	Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
A.12.2 Protección anti malware		
Objetivo: Asegurar la información y las fallas de procesamiento debidas al malware		

A.12.2.1	Controles contra malware	Controles de detección, prevención y recuperación para proteger de malware que sea implementado, combinado con debidas advertencias al usuario
A.12.3 Respaldo		
Objetivo: Protección contra la perdida de datos		
A.12.3.1	Respaldo de información	Respaldar copias de la información, software e imágenes del sistema, las cuales deben ser usadas y evaluadas regularmente según los acuerdos de las políticas.
A.12.4 Monitoreo y Actividad de Usuario		
Objetivo: Grabar eventos y generar evidencia.		
A.12.4.1	Registro y gestión de eventos de actividad	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de los registros de información	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
A.12.4.3	Registros de actividad del administrador y operador del sistema	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
A.12.4.4	Sincronización de relojes	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.
A.12.5 Control de software en ejecución		
Objetivo: Asegurar la integridad de los sistemas en ejecución		
A.12.5.1	Instalación del software en sistemas en producción	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

A.12.6 Gestión de vulnerabilidades técnicas		
Objetivo: Prevenir técnicas de explotación de vulnerabilidades		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
A.12.6.2	Restricciones en la instalación de software	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
A.12.7 Consideraciones de la auditoria de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas de información		
A.12.7.1	Controles de auditoría de los sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
A.13 Seguridad de las telecomunicaciones		
A.13.1 Gestión de seguridad en las redes		
Objetivo: Asegurar la protección de la información en las redes y generar facilidades de procesamiento de la información		
A.13.1.1	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
A.13.1.3	Segregación de redes	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información

A.13.2 Transmisión de información		
Objetivo: Mantener la seguridad en la transmisión de la información entre la organización y una externa.		
A.13.2.1	Políticas y procedimientos de intercambio de información	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos de intercambio	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información referida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad y secreto	se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	La información de los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.

A.14.1.3	Protección de las transacciones por redes telemáticas	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Asegurar la seguridad de la información designada e implementada durante el ciclo de vida del desarrollo de los sistemas de información		
A.14.2.1	Política de desarrollo seguro de software	Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en los sistemas	En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones a los cambios en los paquetes de software	Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
A.14.2.6	Seguridad en entornos de desarrollo	Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que

		abarcan todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Externalización del desarrollo de software	La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
A.14.2.9	Pruebas de aceptación	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
A.14.3 Datos de Prueba		
Objetivo: Asegurar la protección de los datos usados para pruebas		
A.14.3.1	Protección de los datos utilizados en prueba	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.
A.15 Relación con los proveedores		
A.15.1 Seguridad de la información en la relación con los proveedores		
Objetivo: Asegurar la protección de los acuerdos de la organización sean accesibles a los proveedores		
A.15.1.1	Política de seguridad de la información para proveedores	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de proveedores	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los

		riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
A.15.2 Gestión de la prestación de servicios de los proveedores		
Objetivo: La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.		
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información e incidentes		
Objetivo: Asegurar una persistente y efectivo aprovechamiento de la gestión de incidentes de seguridad de información, incluyendo comunicación de las debilidades y sucesión de seguridad		
A.16.1.1	Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.
A.16.1.3	Notificación de puntos débiles de la seguridad	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a

		contratistas que utilizan los sistemas y servicios de información de la organización.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
A.16.1.5	Respuesta a los incidentes de seguridad	Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro
A.16.1.7	Recopilación de evidencias	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.
A.17 Aspectos de la seguridad de la información en la Gestión de la Continuidad de Negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: Determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
A.17.2 Redundancia		
Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de información		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar infracciones de las obligaciones legales, legales, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable	Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.
A.18.1.2	Derechos de propiedad intelectual (DPI)	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.
A.18.1.3	Protección de los registros de la organización	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos,

		normativos, contractuales y comerciales.
A.18.1.4	Protección de datos y privacidad de la información personal	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
A.18.1.5	Regulación de los controles criptográficos	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Se deberían realizar revisiones regulares de la seguridad de los sistemas de información en base a las políticas.		
A.18.2.1	Revisión independiente de la seguridad de la información	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
A.18.2.3	Comprobación del cumplimiento	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Anexo 2: Fichas Técnicas Servidores

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	**DESCRIPCIÓN**
Responsable	Ing. Fernando Garrido
Modelo	IBM System x3500 M4
Memoria RAM	7.6 GB
Disco Duro	610 GB
Interfaces de Comunicación	
Ubicación Física	RACK 3
Función	Repositorio o DSpace
Procesador	Intel Xeon ® CPU E5405 2.0GH x 12
Número de Serie/Identificador UTN	KQ5M81T/1410103.327.0079
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Centos 6.5
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Fernando Garrido
Modelo	IBM System x3500 M4
Memoria RAM	7.6 GB
Disco Duro	135 GB
Interfaces de Comunicación	
Ubicación Física	RACK 3
Función	Reactivos
Procesador	Intel Xeon ® CPU E5405 2.0GH x 12
Número de Serie o Identificador	KQ6M81V/110103.327.0078
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Centos 6.5
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	
Modelo	IBM System x3200 M2
Memoria RAM	2 GB
Disco Duro	1 TB
Interfaces de Comunicación	1 Gigabit Ethernet
Ubicación Física	RACK 2
Función	Radius
Procesador	Dual-core Xeon E3110 3.0
Número de Serie/Identificador UTN	103QCPYOF560/1410107.001.5050
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	Se asignó el servidor inactivo DHCP para utilización de Radius

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Edgar Jaramillo
Modelo	HP Proliant DL 360 G9
Memoria RAM	32 GB
Disco Duro	3x 450 GB
Interfaces de Comunicación	4 x GB
Ubicación Física	RACK 3
Función	Servidor Cloud Open Stack
Procesador	Intel Xeon ® CPU E5-2620 V3
Número de Serie/Identificador UTN	MXQ51704F7/1410107.018.02017
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Edgar Jaramillo
Modelo	ProLiant DL360 Gen 9
Memoria RAM	32 GB
Disco Duro	3x450 GB
Interfaces de Comunicación	4 x 1GBE
Ubicación Física	RACK 2
Función	Servidor Open Nebula
Procesador	Intel Xeon ® CPU E5-2620 V3
Número de Serie/Identificador UTN	MXQ51500L9/1410107.018.02015
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Edgar Jaramillo
Modelo	HP Proliant DL 150 G9
Memoria RAM	4 GB (max)
Disco Duro	160 GB
Interfaces de Comunicación	2 x Gigabit Ethernet
Ubicación Física	RACK 2
Función	Redes SDN
Procesador	Intel Xeon ® CPU E5405 Quad Core
Número de Serie/Identificador UTN	MXS8460A5J/1410107.001.728
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Ubuntu Server 14.04 LTS
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
FICHA TÉCNICA DE SERVIDORES

CARACTERÍSTICAS	DESCRIPCIÓN
Responsable	Ing. Edgar Jaramillo
Modelo	HP Proliant ML 150 G5
Memoria RAM	4.8 GB
Disco Duro	150 GB
Interfaces de Comunicación	
Ubicación Física	RACK 3
Función	Servicio de encuestas y evaluación Opina
Procesador	Intel Xeon ® CPU E54405 GHz x 4
Número de Serie/Identificador UTN	MXS8460A5P/1410107.001.727
Estado	Activo ☐ Inactivo ☐
Sistema Operativo	Ubuntu 12.10
Usuarios Finales	Estudiantes ☐ Profesores ☐ Administrativos ☐
Observaciones	Se plantea la migración del servidor para formar parte de los servidores virtualizados cloud computing

Anexo 3: Políticas De Seguridad Actuales Data-Center

Políticas para Ingreso y Comportamiento de personas al interior del Centro de Datos

El ingreso a un Centro de Datos se considera como restringido, y en la redacción de Políticas de Acceso al mismo, se recomienda incluir los puntos que a continuación se detallan:

- Todo acceso al CDP deberá ser autorizado previamente. El personal encargado deberá estar al tanto de toda solicitud de ingreso al Centro de Datos para su aprobación.

- La(s) personas(s), cuyo acceso al CDP haya sido autorizado, deberá llenar y firmar un formulario donde especifique como mínimo: nombre completo del ingresante, fecha de ingreso, hora de ingreso y salida, actividad realizada dentro del Centro de Datos.

- Códigos, tarjetas de acceso y demás únicamente serán aportados por el personal administrativo encargado del Centro de Datos.

- Está prohibido el ingreso de alimentos o bebidas al interior del CDP. Existen casos donde éstos han provocado, aunque no graves, inconvenientes en el equipamiento TIC.

- No se deberá arrojar ningún tipo de basura en racks, pasillos o piso técnico. La mantención limpia del CDP evitara la emanación de polvo al equipamiento y permitirá el normal flujo del aire en el sistema de refrigeración por todas las dependencias.

- Está terminantemente prohibido fumar o realizar cualquier actividad que provoque la emanación de humo al interior del CDP debido a una posible activación accidental de los sistemas de detección de humo y demás sistemas de seguridad.

- Para visitas técnicas (académicas, inspecciones, o de soporte) se permite el ingreso de grupos de hasta máximo tres personas. Esto debido a que el espacio físico del CDP no es el suficiente y al dimensionamiento del aire acondicionado.
- La puerta de seguridad de ingreso al Data-Center deberá estar cerrada todo el tiempo. No se admite por ningún concepto que se mantenga la puerta ya que esto afecta directamente al funcionamiento del sistema de aire acondicionado.

- Está prohibido apagar el sistema de aire acondicionado cuando ingresen personas al CDP. Las personas deberán conocer, antes de ingresar, las condiciones ambientales en las que trabaja el CDP para evitar cualquier afección que ésta le puede causar.

- Las personas que ingresen al CDP no podrán almacenar ningún tipo de elemento peligroso considerado inflamable como cajas, cartones, papeles o cualquier material similar.

Anexo4: Manual Actual De Procedimiento Para E Ingreso De Personas Al Centro De Datos

1. Realizar una solicitud dirigida al Administrador encargado del CDP en la que se especifique el motivo de la visita, la fecha en la que se la hará y el número de personas que asistirán. Una plantilla válida de la solicitud se muestra en la pág. 211 de este documento.

2. Entrega y lugar

3. Con la solicitud ya en su poder, el Administrador deberá dar aprobación a la misma del(los) solicitante(s). Si la respuesta es negativa, deberá entregarse un comunicado al remitente(s) explicando el motivo de la no aceptación de su ingreso. En caso de una respuesta afirmativa, el Administrador facilitará el formulario de ingreso (Página 212) a la(s) persona(s) para que llenen sus datos personales, teniendo en cuenta siempre lo siguiente:

a. Para visitas académicas se permite el ingreso máximo grupos de 4 personas, incluido el Docente guía o delegado similar. En caso de ser varios los grupos que harán el ingreso, deberán esperar el turno en los pasillos de la Facultad y no en los alrededores de la puerta de acceso del CDP.

b. Para personal técnico que ejecute trabajos de mantenimiento o reparación de la infraestructura, máximo un grupo de 3 personas por tema de manejo de herramientas o procesos similares.

c. Para ingreso de personal de administración y gestión de los equipos TIC, máximo grupos de 3 personas.

4. Al momento de ingresar al Centro de Datos, las personas lo harán en orden, estando siempre atentos a las disposiciones del guía.

a. Para visitas técnicas, no se permitirá el ingreso de: mochilas o bolsos, botellas de bebidas y/o alimentos.

b. Para tareas de mantenimiento físico, al personal no se le permitirá el ingreso de herramientas pesadas que puedan afectar las condiciones físicas del piso técnico o el cableado. En el caso de empleo de herramientas eléctricas, se deberá utilizar el circuito derivado interno, destinado para este fin.

5. Mientras dure la estadía al interior del CDP, está prohibido para las personas: manipular el cableado, presionar botones, abrir puertas de gabinetes, arrojar basura, apoyarse en las estructuras y/o irrumpir en el desempeño normal de los componentes que allí se tiene. La puerta de seguridad deberá estar cerrada todo el tiempo, evitando las fugas de aire.

6. Una vez terminada la visita la(s) persona(s) deberán de igual manera salir en orden, entregando al personal administrador del Data-Center el formulario que recibieron al ingreso, llenando y cumpliendo con toda la información requerida.

Anexo 5: Manual Actual De Procedimiento Actual Para Ingreso De Nuevo Equipamiento TIC

Para instalar nuevo equipamiento TIC en las inmediaciones del Data-Center deberá tomarse en cuenta:

- Justificativo redactado de la necesidad de ingresar el equipamiento a las instalaciones del CDP y las funciones que éste desempeñará.

- Aprobación de la instalación del nuevo equipamiento TIC por parte de la administración del Data-Center, confirmando la disponibilidad y asignación del espacio físico que éste ocupará.

- Autorización de ingreso al personal que realizará la instalación, por parte de la administración del CDP.

- Presentación de garantías del equipamiento y la legalidad del mismo.

- Reporte del funcionamiento, características, configuraciones y estado en el que se encuentra el equipo(s) a ingresar.

- Entrega de los complementos necesarios (cables, tornillos, rieles de soporte, etc.) para la instalación del equipamiento en el CDP.

- En el caso de tener que apagar equipamiento TIC o servidor del CDP, deberá seguir las políticas de “Mantenimiento y Apagado de equipamiento TIC”.

- Registro de actividades realizadas por el personal de instalación que ingresó al CDP en la ficha de control de acceso que se le facilite, completando con todos los datos que en ella se soliciten.

Anexo 6: Manual Actual De Procedimientos De Entrada/Salida De Equipos Del Data-Center Fica

1. Realizar y entregar una solicitud dirigida al Administrador encargado del CDP en la que se justifique el ingreso o salida de equipamiento a la infraestructura del Centro de Datos. Una plantilla válida de la solicitud se muestra en la pág. XXX de este documento.

2. Con la solicitud ya en su poder, el Administrador deberá aprobar o no la solicitud. Si la respuesta es negativa, deberá entregarse un comunicado al remitente(s) explicando el motivo de la no aceptación. En caso de una respuesta afirmativa, el Administrador facilitará el formulario de ingreso o salida de equipos para que sea completado (Formulario de la página XXX). Antes de aceptar la petición, el administrador deberá considerar lo siguiente:

a. EN EL INGRESO DE EQUIPOS: Espacio físico disponible, ubicación que se le asignará al equipo, compatibilidad con las condiciones ambientales y eléctricas de la inmediación.

b. EN LA SALIDA DE EQUIPOS: Nivel en el que afectaría la no presencia del equipo en el CDP y sus posibles consecuencias.

3. Para el ingreso físico y/o salida de equipos se deberá seguir las “políticas de mantenimiento y apagado de equipamiento TIC” y su correspondiente manual de procedimiento.

Anexo 7: Formato Solicitud De Acceso Al Data-Center

UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

SOLICITUD DE INGRESO AL CENTRO DE DATOS FICA

Fecha:	*Fecha de Entrega de la solicitud*
Dirigido a:	*Administrador responsable del CDP*
Solicitante:	*Nombre(s) de todos solicitantes del ingreso*
Facultad:	*Facultad a la que pertenecen el/los solicitante(s)*
Carrera:	*Carrera a la que pertenecen el/los solicitante(s)*
Asunto:	*Motivo de la solicitud para el ingreso*

MOTIVO Y FECHA DE LA VISITA

.....

.....

.....

.....

.....

.....

Atentamente,

FIRMA DEL/LOS SOLICITANTES

CI: XXXXXXXX.X

Anexo 8: Manual De Administrador Firewall

Endian Firewall es un software relativamente completo que lo integran varias herramientas y funcionalidades que se pueden utilizar para implementar políticas en una organización de medio o bajo en su versión community.

Para detallar cada uno de las características se procede a revisar el interfaz web que permite interactuar con la plataforma de manera amigable, en la Figura 54 se puede observar los elementos del panel principal denotados con un cuadro de color rojo y los cuales son:

- Sistema
- Estado
- Red
- Servicios
- Firewall
- Proxy
- VPN
- Registros e informes

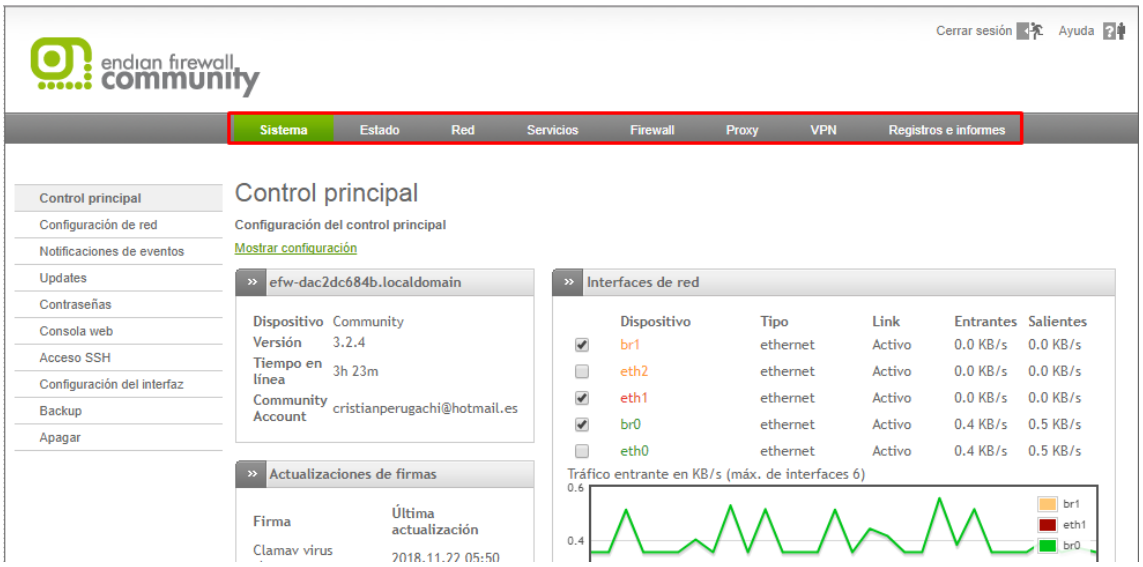


Figura 56. Panel de configuración Endian Firewall
Fuente: Elaborado por el autor

Sistema

Se encuentra en el panel de control y es la porción del software que permite configurar y controlar la parte de funcionalidad de sistema y la parte gráfica. En la figura se puede destacar cada sub-panel o herramientas que integran esta funcionalidad.

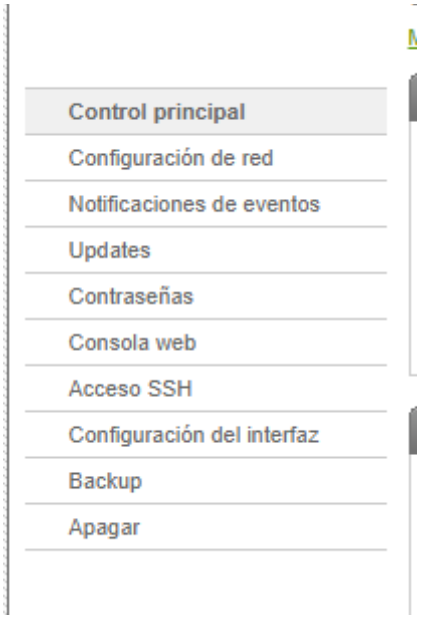


Figura 57. Panel secundario de Sistema
Fuente: Elaborada por el autor

Control Principal: Este panel permite observar ciertas cualidades encontradas en el sistema las que están identificadas en la Figura 56 mediante una numeración que empieza desde el 1 al 5, detallándolas de la siguiente forma:

1) Ventana que indica la versión del software, el tiempo de funcionamiento y el correo con el que se registró.
2) Indica los interfaces de red habilitados, en este caso se puede observar que existe una red WAN (roja), LAN (verde) y DMZ (naranja).
3) Indica el estado y última actualización de la base de datos del antivirus ClamAV
4) Se puede visualizar la información del hardware y el porcentaje de utilización
5) En esta ventana se visualizan los interfaces de red que se encuentran conectados

6) Se puede observar los servicios que se encuentran habilitados de manera resumida.

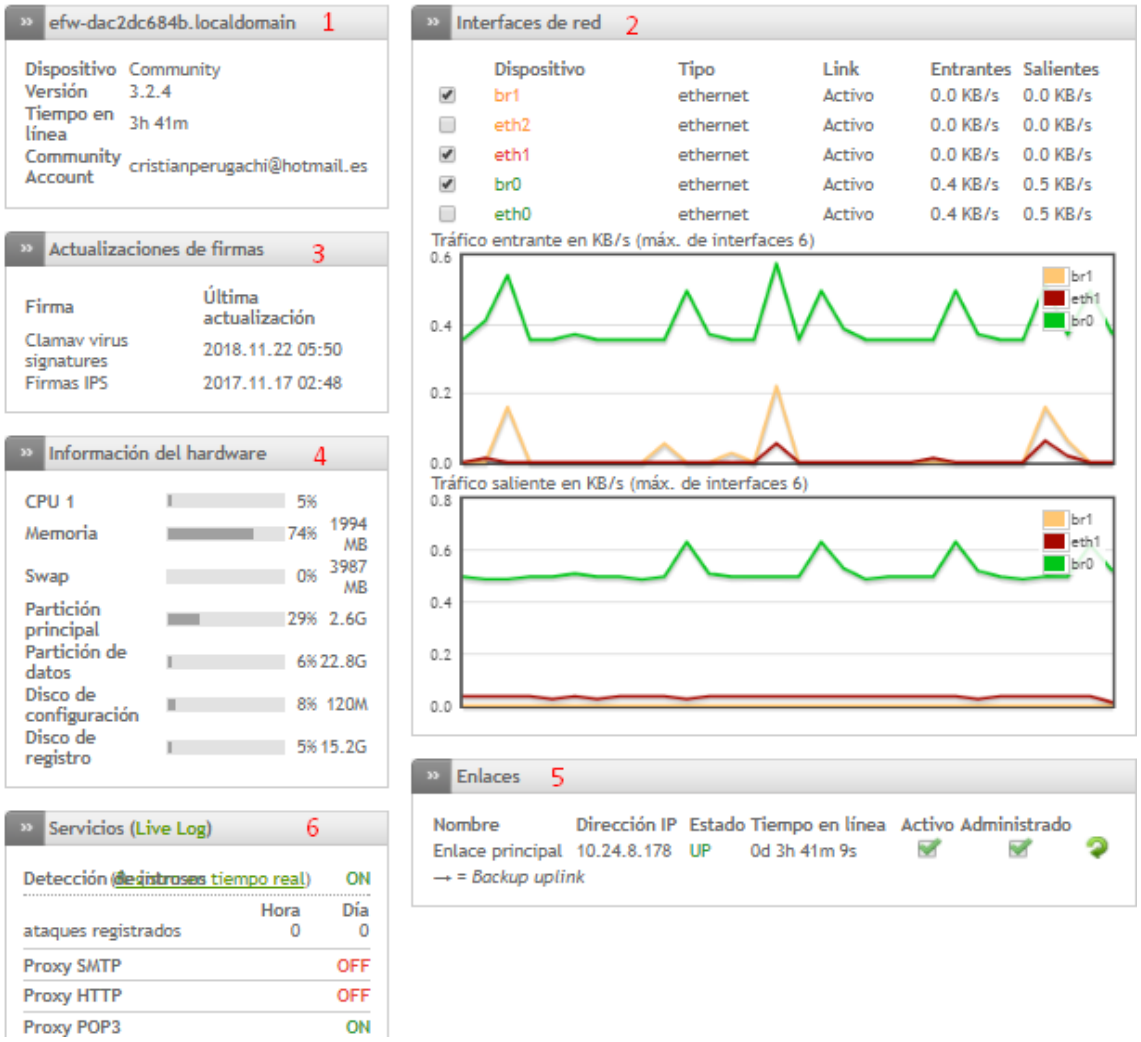


Figura 58. Control principal panel Sistema
Fuente: Elaborado por el autor

Configuración de red: este apartado permite configurar de manera interactiva los interfaces de red disponibles

Figura 59. Configuración de red panel sistema
Fuente: Elaborado por el autor

Como se puede observar en la Figura 57, para la configuración de la red existe un asistente que permite realizar una configuración amigable con el administrador o encargado de la red.

En la figura 58 se puede observar los modos de red que se puede seleccionar, los cuales son: Enrutamiento que permite manejar una segmentación de la red y que el firewall trabaje como un Gateway entre las redes externas e internas; Con puente que permite introducir el software sin modificar la estructura de red y el direccionamiento; Sin enlace que permite que el sistema forme parte de la red local pero no actúa como Gateway.

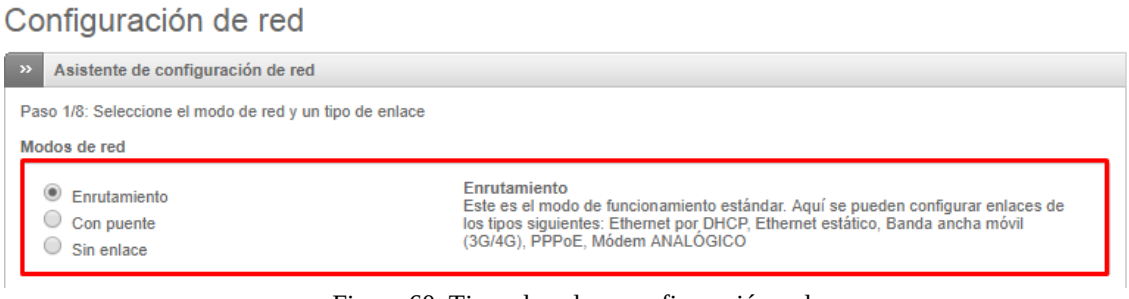


Figura 60. Tipos de enlace configuración red
Fuente: Elaborado por el autor

En el caso de la infraestructura propuesta se seleccionará Ethernet Estático y es necesario definir el tipo de asignación de direccionamiento en la WAN (roja), como se puede ver en la

figura 59 se selecciona Ethernet Estático, pero existen varias opciones entre ellas se encuentran ethernet por DHCP, Banda ancha móvil, PPPoE y modem analógico.

Una vez seleccionada la opción de direccionamiento estático se selecciona siguiente.

Figura 61. Selección tipo de enlace panel Sistema
Fuente: Elaborada por el autor

En la Figura 60, se encuentran detallados los tipos de redes que se pueden configurar en el sistema, para el caso propuesto se configurara la DMZ que representa la red naranja se marca la opción y siguiente.

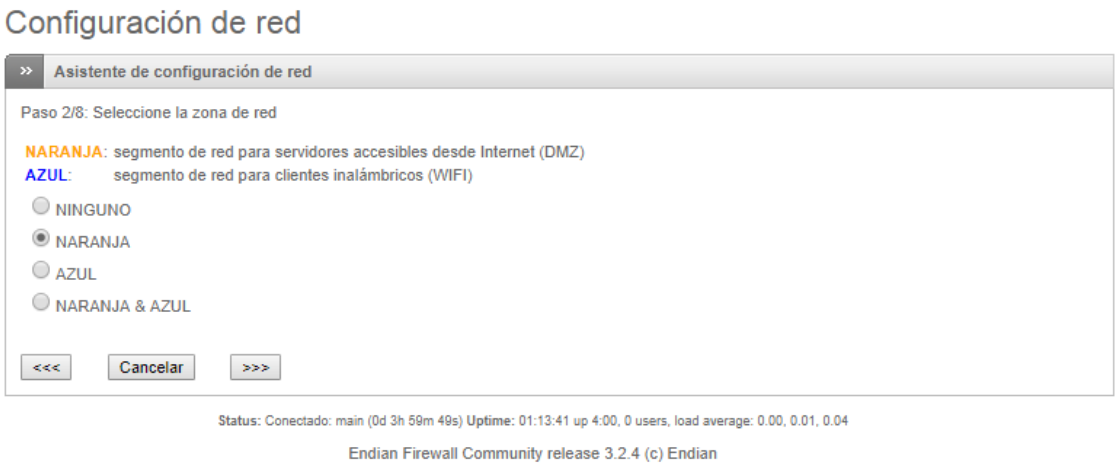


Figura 62. Tipos de redes Naranja o Azul panel sistema
Fuente: Elaborada por el autor

En la figura 61 se procede a configurar las dos redes que son necesarias en la plataforma red LAN(verde) y DMZ (naranja), en cada una se asigna la dirección IP y su máscara de red

además del interfaz físico que se utilizara, una vez completada esta información se selecciona siguiente.

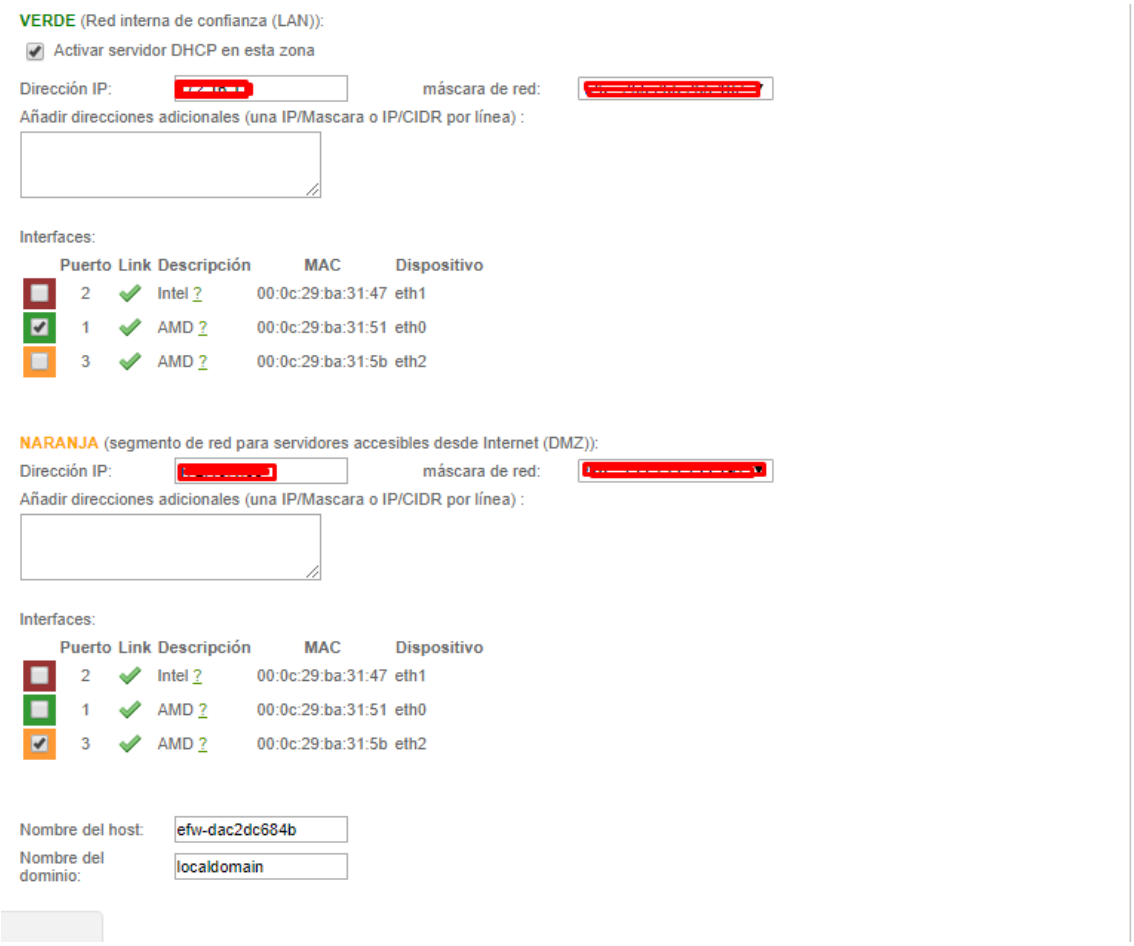


Figura 63. Asignación de interfaz y direccionamiento DMZ y LAN panel sistema
Fuente: Elaborado por el autor

Se procede a configurar la red WAN que tiene el enlace a la red externa para salida a internet y acceso a los servicios desde la internet, como se puede observar en la figura 62 se asigna una dirección IP y su máscara, además de seleccionar el interfaz físico que funcionara como enlace externo.

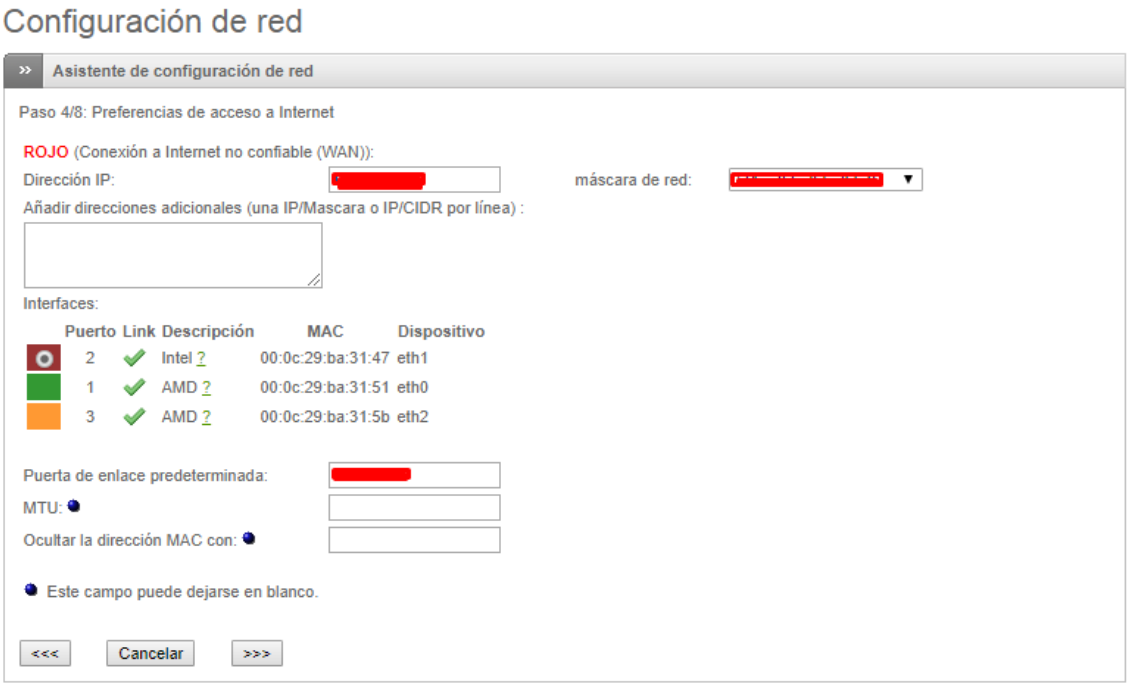


Figura 64. Configuración direccionamiento y Gateway interfaz WAN
Fuente: Elaborada por el autor

Una vez seleccionado siguiente se procede a configurar el DNS de la red WAN (roja) como se puede observar en la Figura 63.

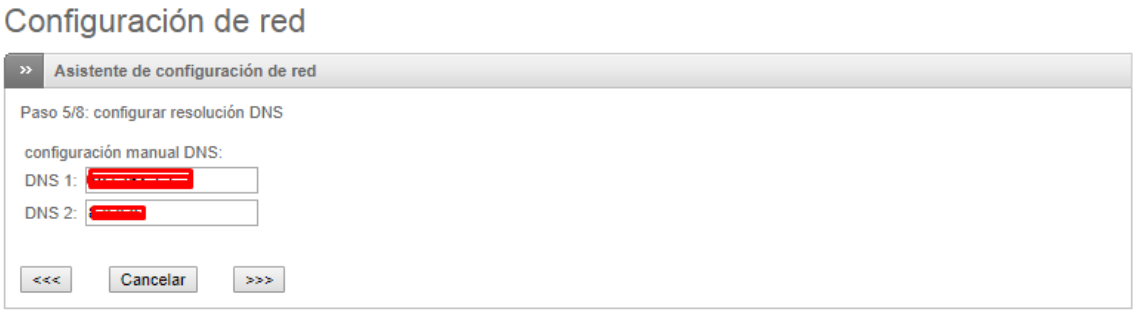


Figura 65. Configuración Gateway interfaz WAN
Fuente: Elaborado por el autor

En caso de tener un servidor de correos interno configurado en la infraestructura se procede a rellenar los campos solicitados en la figura 64.

Figura 66. Configuración servidor de correo
Fuente: Elaborado por el autor

Una vez finalizado la configuración se da click en aceptar la configuración para que se actualicen los interfaces como se puede observar en la figura 65.

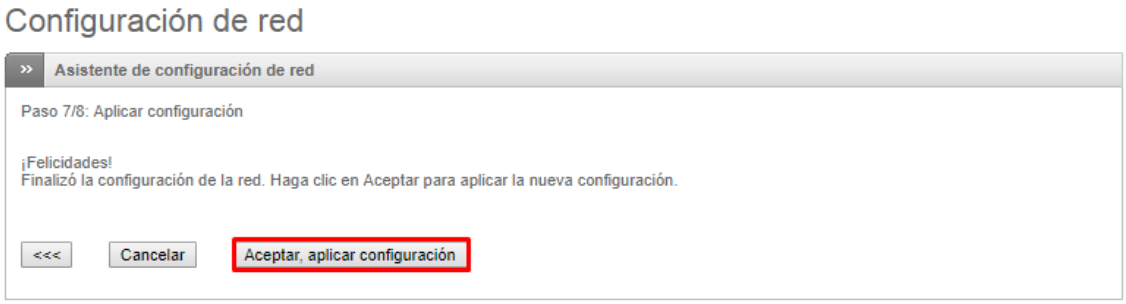


Figura 67. Finalización de configuración de interfaces
Fuente: Elaborado por el autor

Notificación de eventos: Permite que el software informe de los eventos en la seguridad presentados por medio de correo electrónico.

En este apartado se procede a activar la notificación de eventos por medio de un interruptor que se puede observar en la figura 66, en caso de existir un servidor de correo interno se utilizara la configuración previamente ingresada en la figura.

Figura 68. Notificación de eventos
Fuente: Elaborado por el autor

Una vez realizado esta activación se procede a la pestaña de eventos que se puede observar en la figura 67 de donde seleccionar los eventos que se notificaran al administrador de la red teniendo en cuenta varias notificaciones las cuales están activadas en su totalidad para que si existe un fallo físico o lógico se notifique por mail al encargado.

Figura 69. Eventos configurados para notificar
Fuente: Elaborado por el autor

Updates: este apartado permite actualizar las herramientas integradas en Endian firewall por medio del registro de un correo como se puede observar en la figura 68, una vez realizado se conecta al interfaz por medio de ssh y se introduce el comando efw-upgrade.

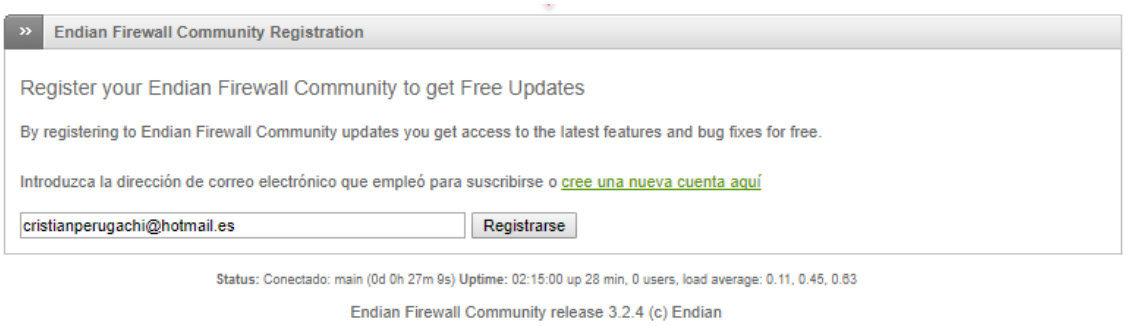


Figura 70. Registro del software
Fuente: Elaborado por el autor

Contraseñas: Esta sección permite modificar la contraseña que viene por defecto en interfaz web y root que viene establecida como endian. En la figura 69 se puede observar el apartado una vez cambiada la contraseña se hace click en cambiar contraseña, la página se reinicia y solicita las nuevas credenciales.

Figura 71. Cambio de contraseñas
Fuente: Elaborado por el autor

Consola web: Como se puede observar en la figura 70 es un terminar en la plataforma web que permite acceder al sistema de forma remota por medio del promt.

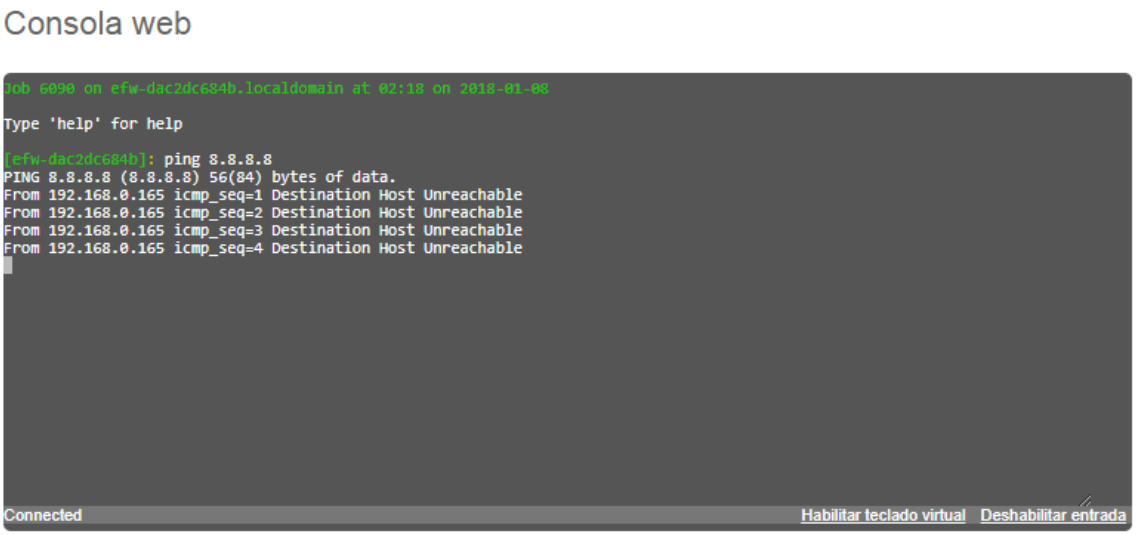


Figura 72. Consola web al promt
Fuente: Elaborado por el autor

Acceso SSH: Se debe configurar el acceso SSH por medio de la pestaña observada en la figura 71, además se puede permitir el acceso tanto como por contraseña de root o por medio de clave publica para darle mayor seguridad.

Figura 73. Configuración Gateway interfaz WAN
Fuente: Elaborado por el autor

Configuración del interfaz: Este segmento permite configurar el idioma del sistema como se puede observar en la figura 72, para este caso se selecciona español y se da click en guardar.

Figura 74. Configuración idioma del interfaz
Fuente: Elaborado por el autor

Backup: Se puede crear un respaldo de la configuración del firewall dentro de este apartado como se puede observar en la figura 73 existen dos pestañas que son backup y backup programado.

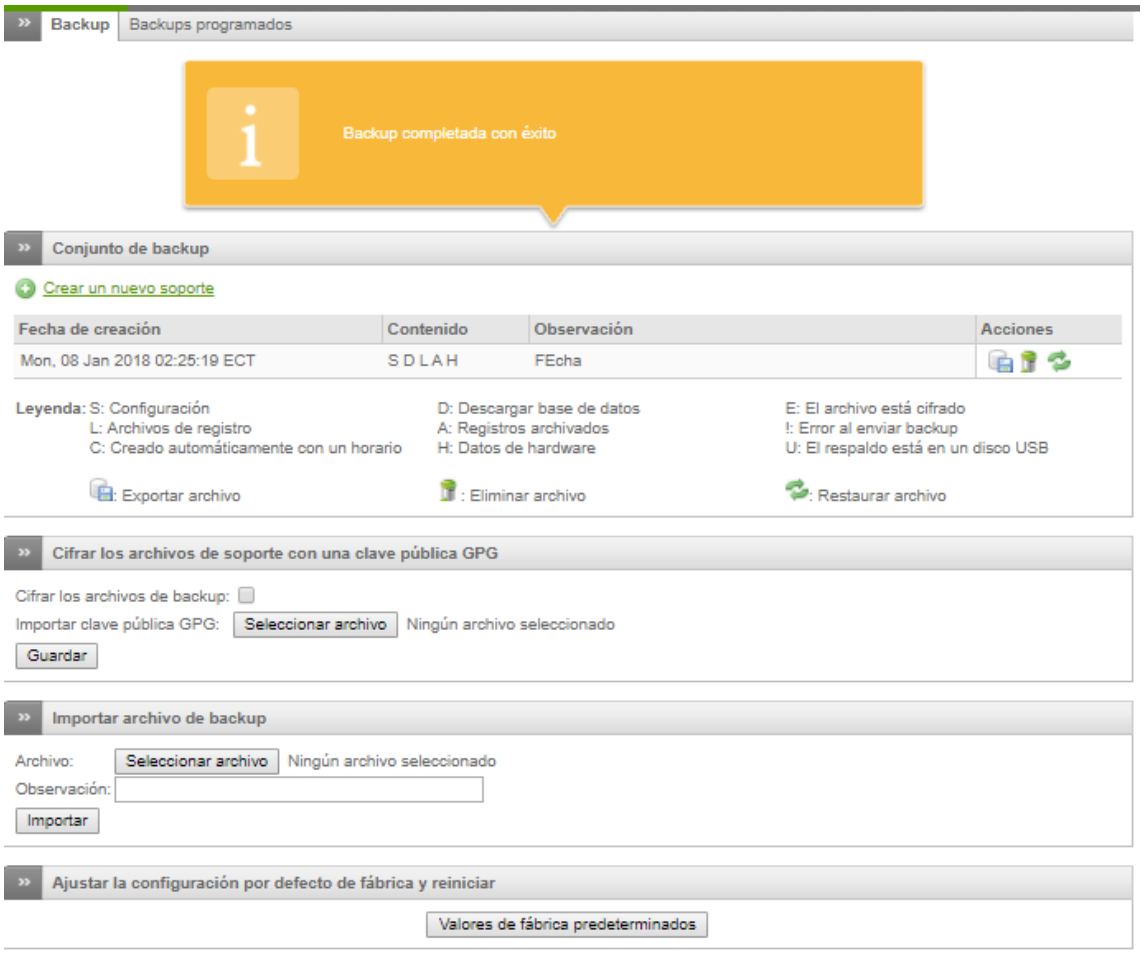


Figura 75. Configuración Backup
Fuente: Elaborado por el autor

Dentro de backup están dividas en segmentos que son: conjunto de backup, cifrar los archivos de soporte con clave publica e importar archivo de backup.

En la figura 73 se puede observar que para crear un nuevo soporte o respaldo hay un texto en letra verde, se hace click y se accede a las opciones de respaldo que se observan en la figura 74.

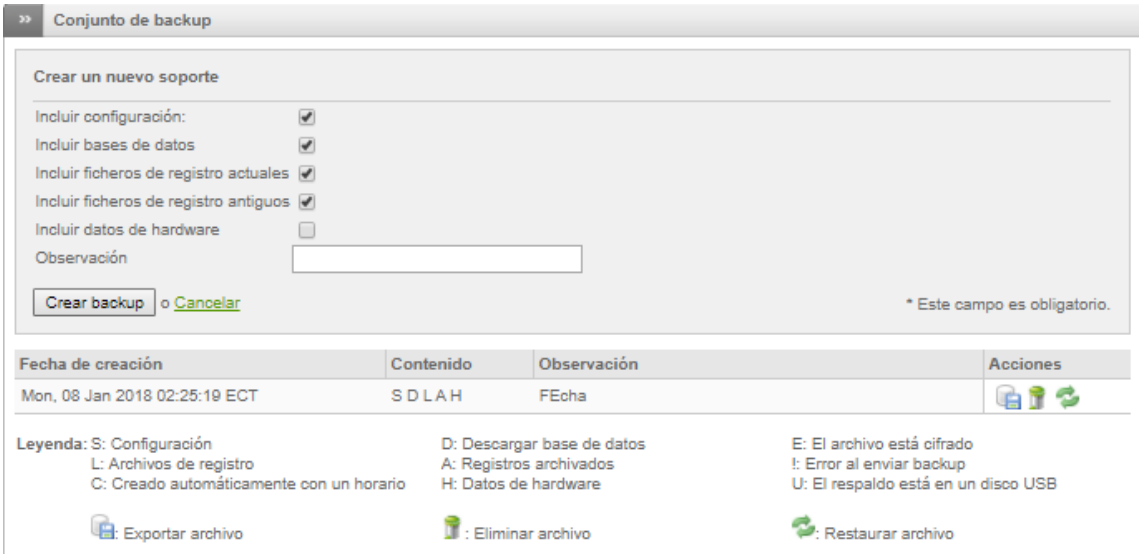


Figura 76. Crear backup
Fuente: Elaborado por el autor

Una vez seleccionado las opciones con un visto en el casillero donde se puede incluir configuración, bases de datos, ficheros de registro y datos de hardware se selecciona crear, esperamos un momento como se puede observar en la figura 75 mientras se aplican los cambios.

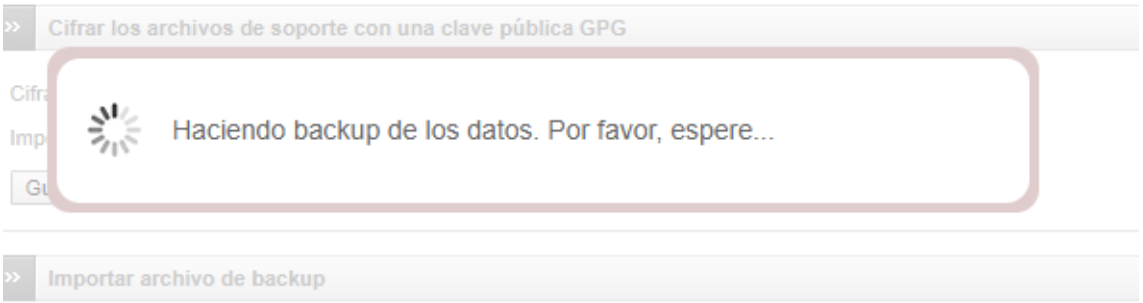


Figura 77. Pantalla espera elaboración backup
Fuente: Elaborado por el autor

En la figura 76 se puede visualizar el backup creado con las opciones permitidas que son: exportar, eliminar y restaurar.

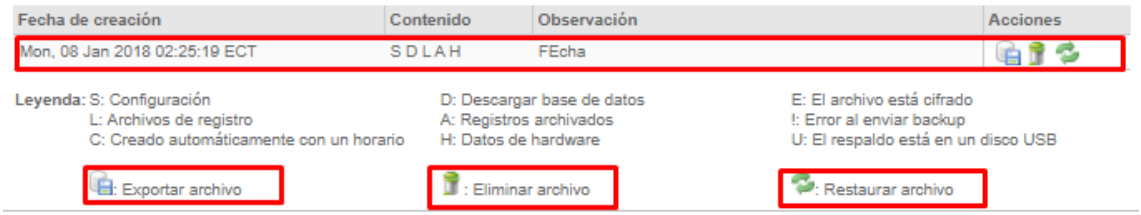


Figura 78. Visualización de backup creado
Fuente: Elaborado por el autor

Para importar solo damos click seleccionar archivo, una vez seleccionado en importar como se puede observar en la figura 77.

Figura 79. Importar backup
Fuente: Elaborado por el autor

Una vez finalizado la importación los valores se configurarán en base al respaldo creado permitiendo migrar de un equipo a otro la configuración de manera rápida y eficiente.

Dentro de la opción de backup programado se puede seleccionar cada cuanto se realizará un backup automático y las opciones que se respaldaran, además también se puede enviar el respaldo al correo del administrador en caso de contar con un servidor de correos configurado. Todo lo descrito se puede observar en la figura 78.

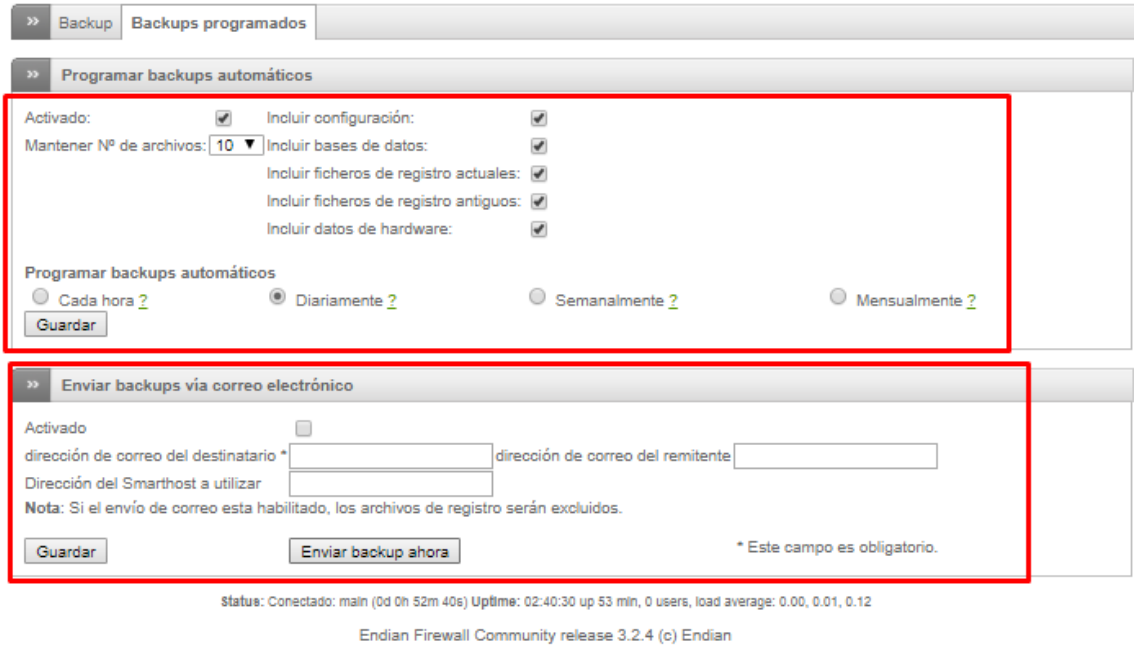


Figura 80. Programación de backup
Fuente: Elaborado por el autor

Apagar: La última opción de esta sección es apagar en donde se puede seleccionar apagar el sistema o reiniciarlo como se puede observar en la figura.

Figura 81. Apagar o reinicia Endian Firewall
Fuente: Elaborado por el autor

Estado

En la porción del panel principal se puede encontrar este ítem que nos permite visualizar el estado del sistema por medio de monitores que se presentan de manera organizada en este apartado.

Información del estado del sistema: Este sub-panel permite visualizar las funcionalidades del sistema que son: Servicios (Figura 80), memoria (Figura 81), uso de disco (Figura 82), Tiempo de acceso host (Figura 83), Módulos cargados (Figura 84) y versión kernel (Figura 85).

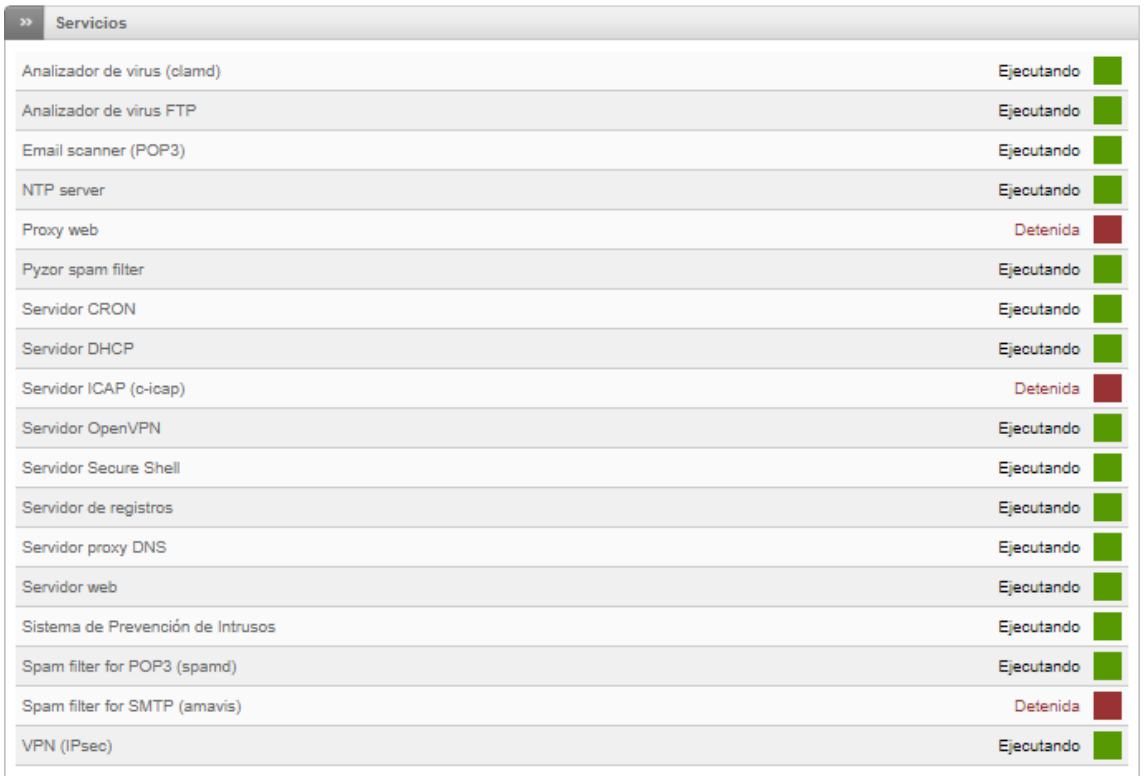


Figura 82. Estado servicios
Fuente: Elaborado por el autor

Figura 83. Memoria Endian Firewall
Fuente: Elaborado por el autor

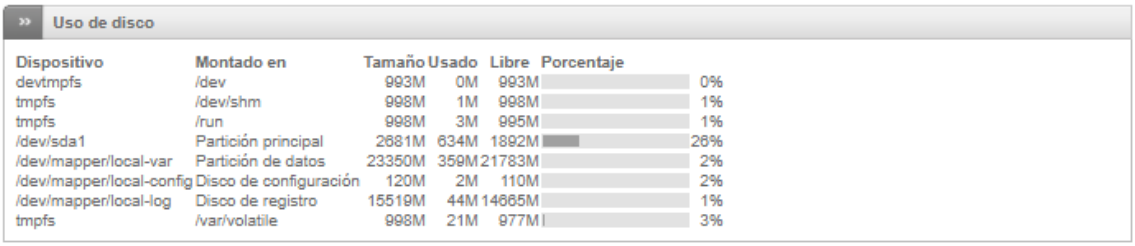
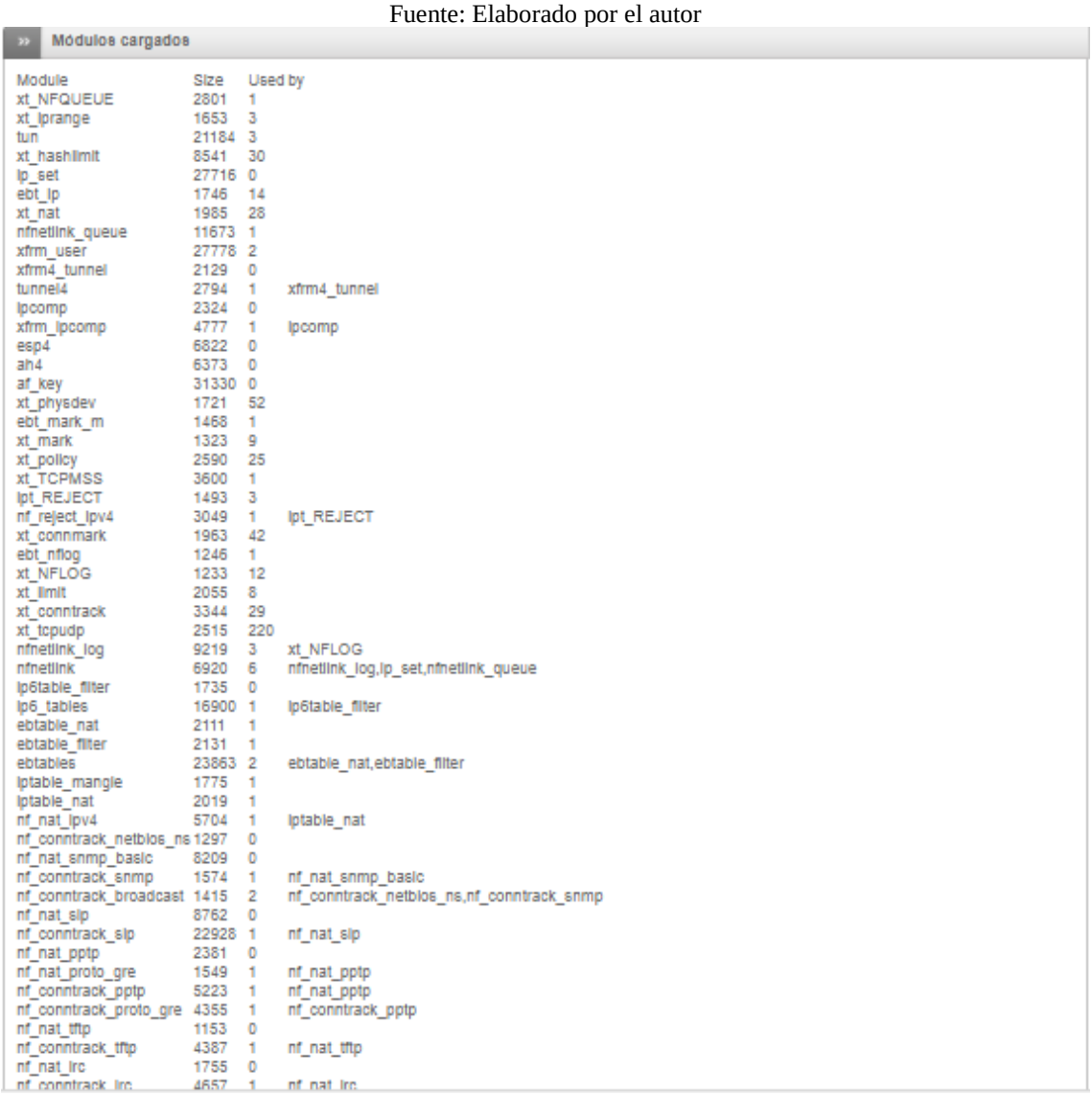


Figura 84. Uso de disco Endian firewall
Fuente: Elaborado por el autor

Figura 85. Tiempo de servicio y usuarios

Fuente: Elaborado por el autor



Módulos cargados

Module	Size	Used by
xt_NFQUEUE	2801	1
xt_iprange	1653	3
tun	21184	3
xt_hashlimit	8541	30
ip_set	27716	0
ebt_ip	1746	14
xt_nat	1985	28
nfnetlink_queue	11673	1
xfrm_user	27778	2
xfrm4_tunnel	2129	0
tunnel4	2794	1 xfrm4_tunnel
ipcomp	2324	0
xfrm_ipcomp	4777	1 ipcomp
esp4	6822	0
ah4	6373	0
af_key	31330	0
xt_physdev	1721	52
ebt_mark_m	1468	1
xt_mark	1323	9
xt_policy	2590	25
xt_TCPMSS	3600	1
ipt_REJECT	1493	3
nf_reject_ipv4	3049	1 ipt_REJECT
xt_connmark	1963	42
ebt_nflog	1246	1
xt_NFLOG	1233	12
xt_limit	2055	8
xt_conntrack	3344	29
xt_tcpudp	2515	220
nfnetlink_log	9219	3 xt_NFLOG
nfnetlink	6920	6 nfnetlink_log,ip_set,nfnetlink_queue
ip6table_filter	1735	0
ip6_tables	16900	1 ip6table_filter
ebtable_nat	2111	1
ebtable_filter	2131	1
ebtables	23863	2 ebtable_nat,ebtable_filter
iptable_mangle	1775	1
iptable_nat	2019	1
nf_nat_ipv4	5704	1 iptable_nat
nf_conntrack_netbios_ns	1297	0
nf_nat_snmp_basic	8209	0
nf_conntrack_snmp	1574	1 nf_nat_snmp_basic
nf_conntrack_broadcast	1415	2 nf_conntrack_netbios_ns,nf_conntrack_snmp
nf_nat_sip	8762	0
nf_conntrack_sip	22928	1 nf_nat_sip
nf_nat_pptp	2381	0
nf_nat_proto_gre	1549	1 nf_nat_pptp
nf_conntrack_pptp	5223	1 nf_nat_pptp
nf_conntrack_proto_gre	4355	1 nf_conntrack_pptp
nf_nat_tftp	1153	0
nf_conntrack_tftp	4387	1 nf_nat_tftp
nf_nat_irc	1755	0
nf_conntrack_irc	4657	1 nf_nat_irc

Figura 86. Módulos cargados
Fuente: Elaborado por el autor

Versión del Kernel

```
4.1.35.e14.1
```

Figura 87. Versión Kernel
Fuente: Elaborado por el autor

Cada una de estas funcionalidades permiten revisar de manera permanente la situación del sistema de forma generalizada.

Estado de la red: En este segmento es posible visualizar la situación de la red, direccionamiento, direcciones físicas, asignaciones dinámicas, estado de la NIC, tabla de

enrutamiento y tabla arp es decir todo lo referente a la parte física como lógica de los interfaces de red como se puede observar en la Figura 86 y la Figura 87.

Interfaces

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UNKNOWN qlen 1000
    link/ether 00:0c:29:ba:31:51 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:ba:31:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.165/24 brd 192.168.0.255 scope global eth1
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br1 state UP qlen 1000
    link/ether 00:0c:29:ba:31:5b brd ff:ff:ff:ff:ff:ff
6: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:0c:29:ba:31:5b brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.65/26 brd 172.16.1.127 scope global br1
       valid_lft forever preferred_lft forever
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:0c:29:ba:31:51 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.1/26 brd 172.16.1.63 scope global br0
       valid_lft forever preferred_lft forever
8: tap0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP qlen 100
    link/ether e6:ca:57:62:81:80 brd ff:ff:ff:ff:ff:ff
```

Figura 88. Estado interfaces de red de Endian Firewall
Fuente: Elaborado por el autor

Asignaciones dinámicas actuales

#	Dirección IP	Dirección MAC	Nombre del host	Caducidad de asignación (local time d/m/y)
1	172.16.1.3	00:0c:29:ba:b6:ee		~~22/11/2017 03:57:00~~

Estado de NIC

```
2) eth1: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01) - 00:0c:29:ba:31:47 [Enlace correcto]
   Velocidad: 1000Mb/s  Completo Doble
   Soporte para negociación automática: Sí  Publicitado  Activado
   Modos de enlaces publicitados:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Modos de enlaces compatibles:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
1) eth0: AMD [Advanced Micro Devices, Inc.] 79c970 [PCnet32 LANCE] (rev 10) - 00:0c:29:ba:31:51 [Enlace correcto]
   Modos de enlaces publicitados:
   Modos de enlaces compatibles:
3) eth2: AMD [Advanced Micro Devices, Inc.] 79c970 [PCnet32 LANCE] (rev 10) - 00:0c:29:ba:31:5b [Enlace correcto]
   Modos de enlaces publicitados:
   Modos de enlaces compatibles:
```

Entradas de la tabla de enrutamiento

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth1
172.16.1.0      0.0.0.0         255.255.255.192 U     0      0        0 br0
172.16.1.64     0.0.0.0         255.255.255.192 U     0      0        0 br1
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

Entradas de la tabla ARP

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.1                      (incomplete)                              eth1
172.16.1.2               ether   00:50:56:c0:00:02   C                     br0
```

Figura 89. Estado NIC, tabla de enrutamiento, tabla ARP
Fuente: Elaborado por el autor

Gráficos del sistema: como se observa en la Figura 88 permite visualizar de manera gráfica como están trabajando el CPU, la memoria ram y el swap permitiendo que se controle en tiempo real el procesamiento de cada uno de ellos.

Figura 90. Configuración Gateway interfaz WAN
Fuente: Elaborado por el autor

Gráficos del tráfico: como se observa en la figura 89 se puede visualizar el tráfico en tiempo real que atraviesa cada uno de los interfaces o redes creadas en el software Endian Firewall.

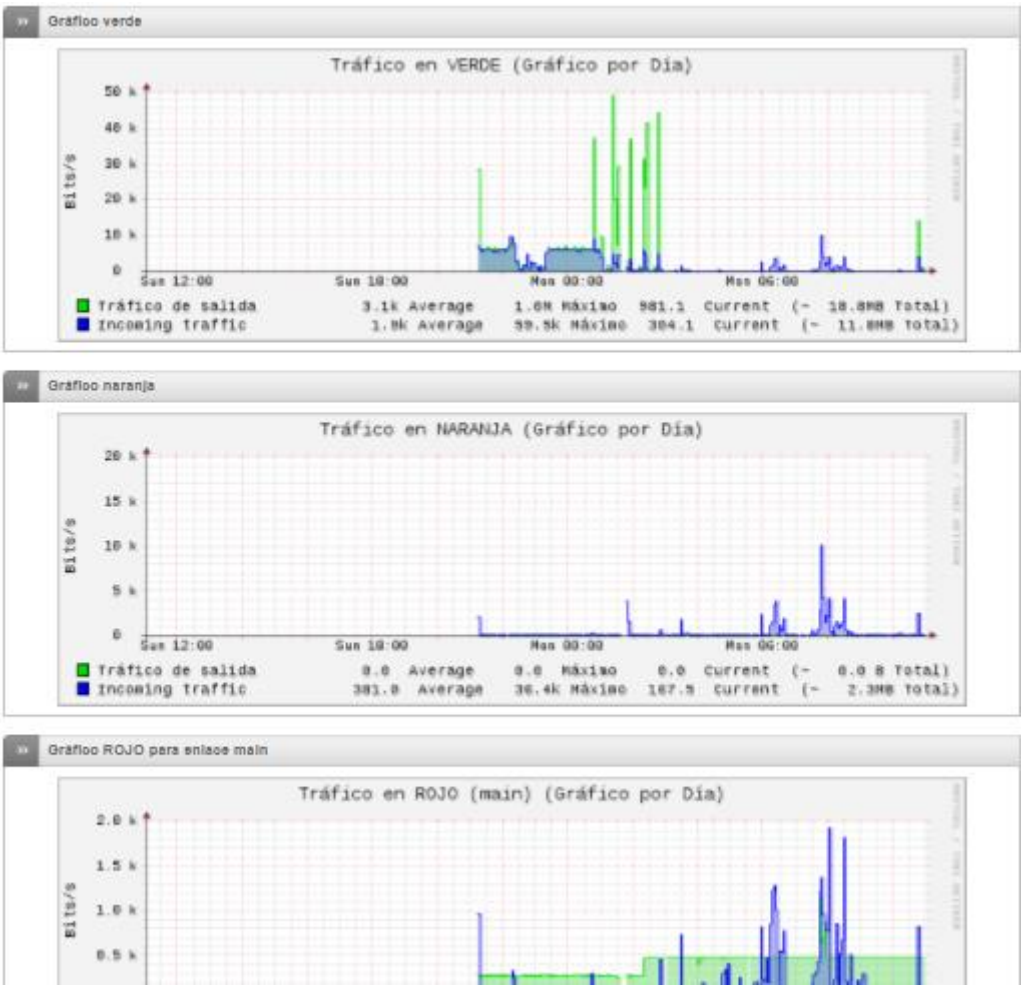
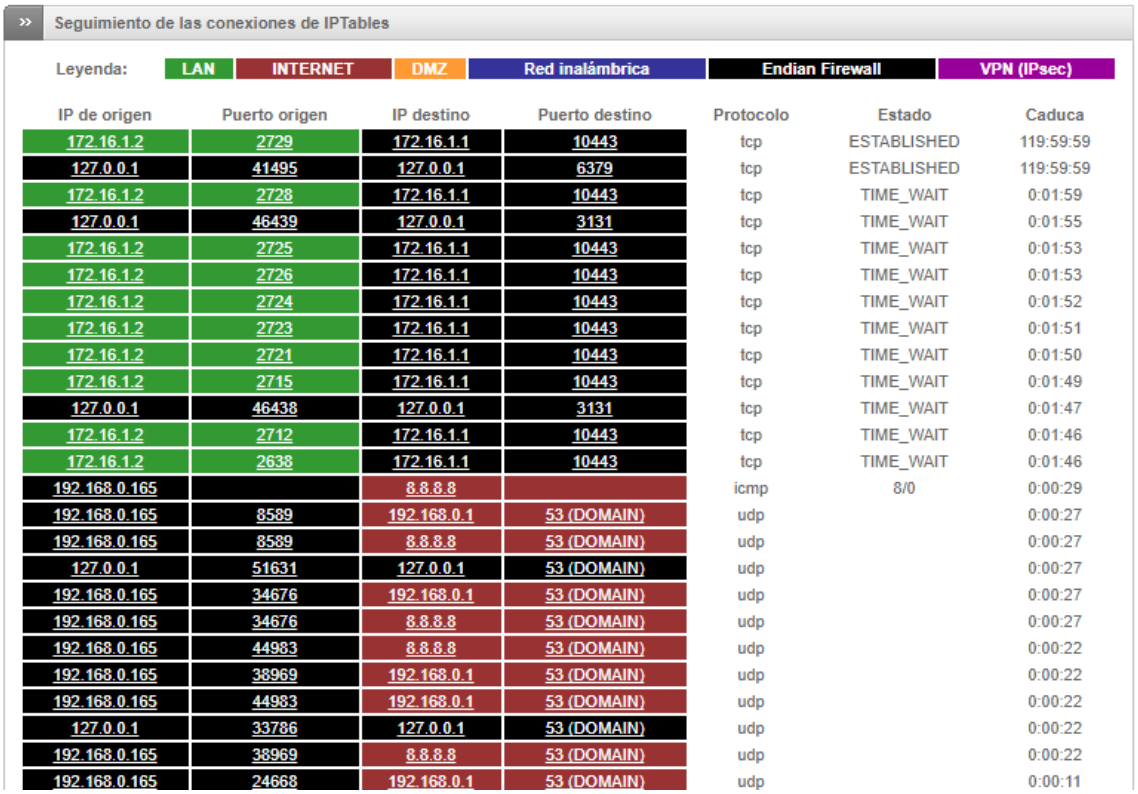


Figura 91. Grafio trafico redes activas Endian Firewall
Fuente: Elaborado por el autor

Conexiones: Permite visualizar la aplicación de las IPtables o reglas de enrutamiento asignadas en el Firewall como se observa en la Figura 90.



IP de origen	Puerto origen	IP destino	Puerto destino	Protocolo	Estado	Caduca
172.16.1.2	2729	172.16.1.1	10443	tcp	ESTABLISHED	119:59:59
127.0.0.1	41495	127.0.0.1	6379	tcp	ESTABLISHED	119:59:59
172.16.1.2	2728	172.16.1.1	10443	tcp	TIME_WAIT	0:01:59
127.0.0.1	46439	127.0.0.1	3131	tcp	TIME_WAIT	0:01:55
172.16.1.2	2725	172.16.1.1	10443	tcp	TIME_WAIT	0:01:53
172.16.1.2	2726	172.16.1.1	10443	tcp	TIME_WAIT	0:01:53
172.16.1.2	2724	172.16.1.1	10443	tcp	TIME_WAIT	0:01:52
172.16.1.2	2723	172.16.1.1	10443	tcp	TIME_WAIT	0:01:51
172.16.1.2	2721	172.16.1.1	10443	tcp	TIME_WAIT	0:01:50
172.16.1.2	2715	172.16.1.1	10443	tcp	TIME_WAIT	0:01:49
127.0.0.1	46438	127.0.0.1	3131	tcp	TIME_WAIT	0:01:47
172.16.1.2	2712	172.16.1.1	10443	tcp	TIME_WAIT	0:01:46
172.16.1.2	2638	172.16.1.1	10443	tcp	TIME_WAIT	0:01:46
192.168.0.165		8.8.8.8		icmp	8/0	0:00:29
192.168.0.165	8589	192.168.0.1	53 (DOMAIN)	udp		0:00:27
192.168.0.165	8589	8.8.8.8	53 (DOMAIN)	udp		0:00:27
127.0.0.1	51631	127.0.0.1	53 (DOMAIN)	udp		0:00:27
192.168.0.165	34676	192.168.0.1	53 (DOMAIN)	udp		0:00:27
192.168.0.165	34676	8.8.8.8	53 (DOMAIN)	udp		0:00:27
192.168.0.165	44983	8.8.8.8	53 (DOMAIN)	udp		0:00:22
192.168.0.165	38969	192.168.0.1	53 (DOMAIN)	udp		0:00:22
192.168.0.165	44983	192.168.0.1	53 (DOMAIN)	udp		0:00:22
127.0.0.1	33786	127.0.0.1	53 (DOMAIN)	udp		0:00:22
192.168.0.165	38969	8.8.8.8	53 (DOMAIN)	udp		0:00:22
192.168.0.165	24668	192.168.0.1	53 (DOMAIN)	udp		0:00:11

Figura 92. Visualización aplicación IPtables
Fuente: Elaborado por el autor

Servicios

En este segmento del panel principal se puede configurar los principales servicios que integran el software Endian firewall.

Servidor DHCP: Se puede configurar un servidor DHCP para cada uno de los interfaces tanto LAN, DMZ o red inalámbrica. Para realizarlo lo primero que se realiza como se puede observar en la figura 91 es seleccionar el interfaz.

Figura 93. Selección de interface configuración DHCP
Fuente: Elaborado por el autor

Una vez seleccionada y habilitada la pestaña del interfaz se procede a hacer click en configuración presentándose la siguiente ventana como se observa en la Figura 92, en donde se asignará tanto la dirección de inicio y fin para asignación del DHCP o mejor conocido como rango, además de los servidores DNS.

Figura 94. Configuración DHCP
Fuente: Elaborado por el autor

Motor antivirus: Esta sección permite habilitar el antivirus integrado para control de tráfico en los servidores internos de correo o ftp en caso de existir, su configuración se puede observar en la figura 93.

Figura 95. Configuración ClamAV
Fuente: Elaborado por el autor

Al configurar hay que tener en cuenta los parámetros de revisión que permitan manejar el tráfico de datos en base a las condiciones de la organización.

Servidor NTP: Dentro de las funcionalidades de Endian Firewall es posible configurar un servidor que ajusta la hora de los servidores enlazados a la infraestructura de red de la organización, para configurar solo es necesario habilitar las opciones presentadas en la figura 94, en donde se puede sobrescribir los servidores NTP de cada uno de los equipos controlados.

Figura 96. Configuración servidor NTP
Fuente: Elaborado por el autor

Aprendizaje de spam: Este apartado permite de forma automática configurar un servidor de autoaprendizaje de spam, cada uno de los procesos que afecten como spam en la red será aprendido y bloqueado en futuros incidentes ocasionados. En la figura 95 se puede observar las opciones para configurar todas las funcionalidades necesarias, aunque la configuración por defecto es la óptima para una organización de tamaño medio.

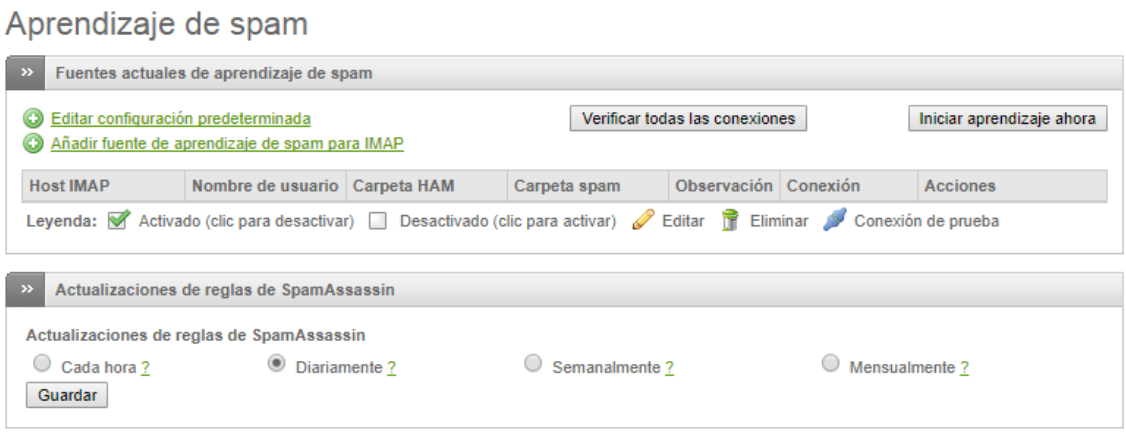


Figura 97. Configuración Aprendizaje SPAM
Fuente: Elaborado por el autor

Prevención de intrusos: Se activa el servidor de prevención de intrusos que es controlado por la herramienta SNORT la cual por defecto viene enlazada a las bases de datos de la herramienta permitiendo mantener de manera constante actualizaciones de reglas de acceso y listas negras de todas las organizaciones en el mundo que utilizan este paquete de prevención de intrusos. Esta utilidad se habilita solo seleccionando el interruptor que se

encuentra en la figura 96 y es utilizado para evitar riesgos reportados con anterioridad y actualización constante de repositorios de reglas de acceso y bloqueo de páginas reportadas como amenazas lo que se puede ver en la figura 97.

Figura 98. Configuración IPS con motor de reglas SNORT
Fuente: Elaborado por el autor

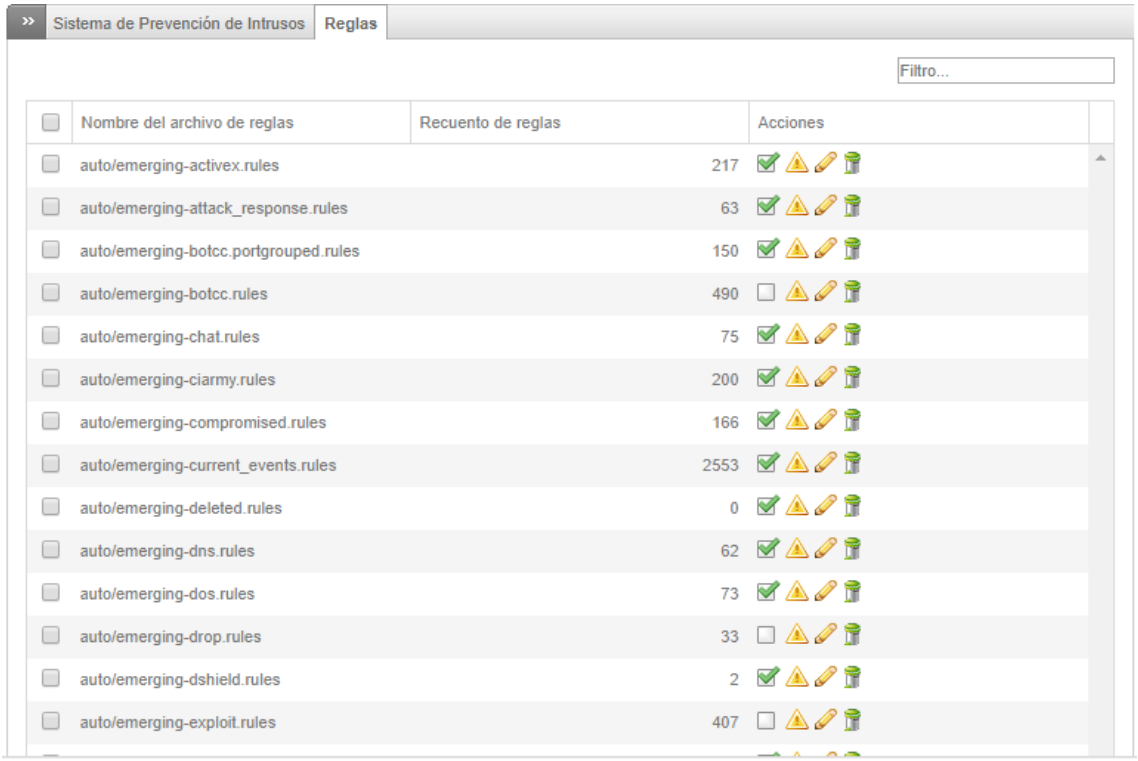


Figura 99. Reglas Activas SNORT
Fuente: Elaborado por el autor

Monitorización del Trafico: Permite habilitar la herramienta NTOP para visualizar el tráfico y las interacciones de los hosts en la infraestructura controlada por Endian Firewall, como se puede observar en la Figura 98.

Figura 100. Habilitar NTOP
Fuente: Elaborado por el autor

En caso de querer utilizar un servidor SNMP para el control y monitorización de la red de manera específica para cada uno de los servidores integrados las opciones vienen

configuradas por defecto y solo es necesario habilitar el servicio como se observa en la figura 99.

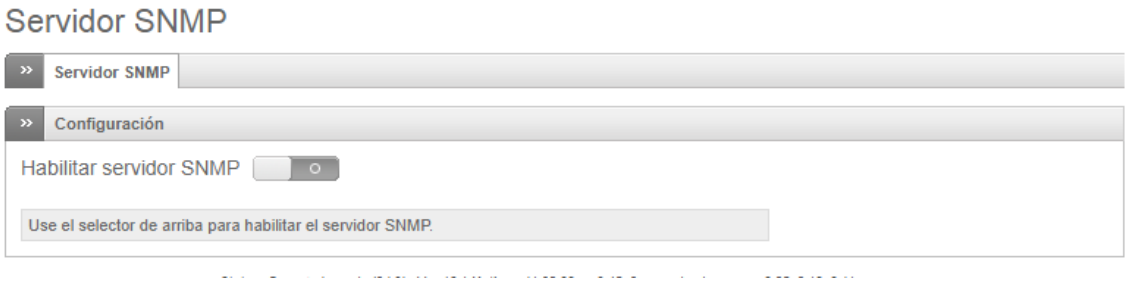


Figura 101. Configuración servidor SNMP
Fuente: Elaborado por el autor

Calidad de servicio: Permite configurar host o servidores para asignación de prioridades en la infraestructura en caso de requerir ciertos servidores se procederá a darles prioridad máxima, media o baja y de esta manera optimizar el peticiona miento y evitar caídas críticas de servicios importantes.

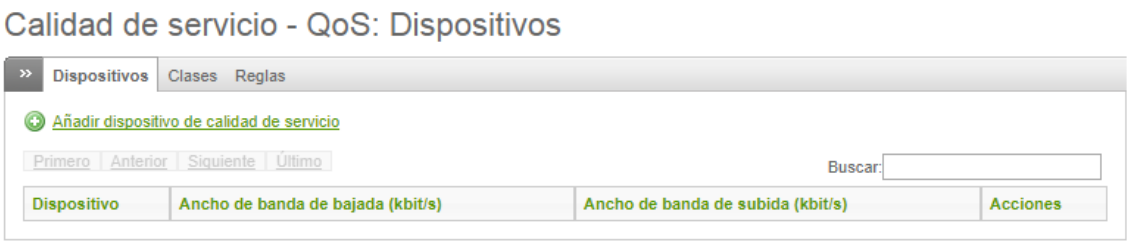


Figura 102. Configuración Gateway interfaz WAN
Fuente: Elaborado por el autor

Como se puede observar en la Figura 100 se agrega el host en la porción de dispositivos, la clase que permite asignar una prioridad desde el 1 al 10 siendo 10 la máxima prioridad y luego las reglas de acceso que vendría a ser una IPtable que especifica el funcionamiento del servicio dependiendo de la prioridad asignada.

Firewall

Esta porción del software es la base de todo el sistema porque se encarga de crear las reglas de acceso y reglas de NAT para el acceso externo e interno a los servidores y servicios en la figura 101 se puede observar las funcionalidades que presenta este elemento.

Figura 103. Interfaz panel firewall
Fuente: Elaborado por el autor

Redirección de puertos NAT: en esta sección como se puede apreciar en la figura 102 se encuentran detallados las reglas para permitir el acceso a los servidores alojados en la DMZ desde internet.

Figura 104. Configuración redirección de puertos NAT
Fuente: Elaborado por el autor

Para agregar un nuevo servidor solo es necesario hacer click en Agregar nueva regla y llenar los parámetros solicitados en la ventana que se muestra en la figura 103, en donde se

solicita la dirección de entrada o IP de WAN, el servicio o puerto asignado y la traducción al puerto y dirección IP del servidor en la DMZ.

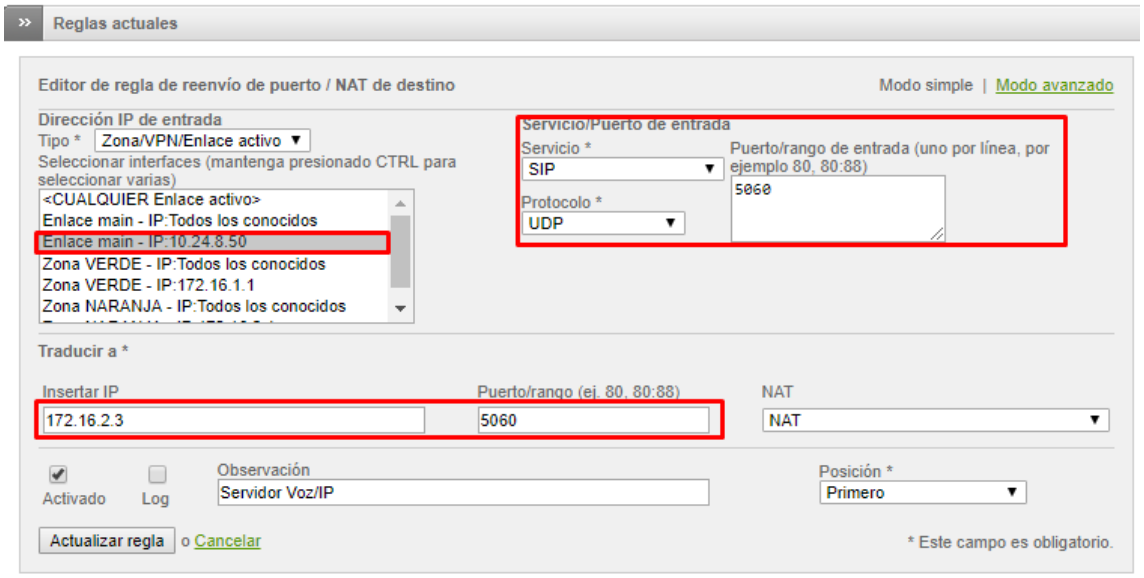


Figura 105. Configuración NAT
Fuente: Elaborado por el autor

Además, como se observa en la figura 104 existe la pestaña de NAT de fuente que permite enmascarar las redes internas para que no sean accesibles desde la red externa, y que permitan el acceso solo en caso de ser autorizado por el administrador.

Figura 106. Configuración NAT de fuente
Fuente: Elaborado por el autor

En este apartado se encuentra también la opción de trafico de enrutado en la figura 105 se puede observar cómo se aplican reglas de acceso remoto para limitar el acceso a puertos solo por medio de una IP que se asignara al administrador.

Figura 107. Configuración tráfico enrutado de entrada
Fuente: Elaborado por el autor

Firewall de salida: Son todas las reglas que se pueden configurar para acceso desde la red interna hacia la externa, por defecto todos los puertos protocolos y servicios están bloqueados desde DMZ y LAN hacía la WAN, pero para la navegación de internet y manejo de ciertos servicios de descarga correo y resolución de nombres es necesario habilitar reglas que permitan actualizar los servidores o aceptar la navegación de los usuarios de redes LAN. En la figura 106 se puede observar las reglas que se implementan para habilitar la navegación de la red LAN.

Figura 108. Configuración firewall de salida
Fuente: Elaborado por el autor

Para añadir nuevas reglas se selecciona añadir nueva regla al firewall y se desplegara una pestaña de configuración como se observa en la figura 107 la cual solicita la red interna de origen, la red destino, el puerto o protocolo permitido, el tipo de política si es de aceptación o denegación y una observación para detallar la regla implementada.

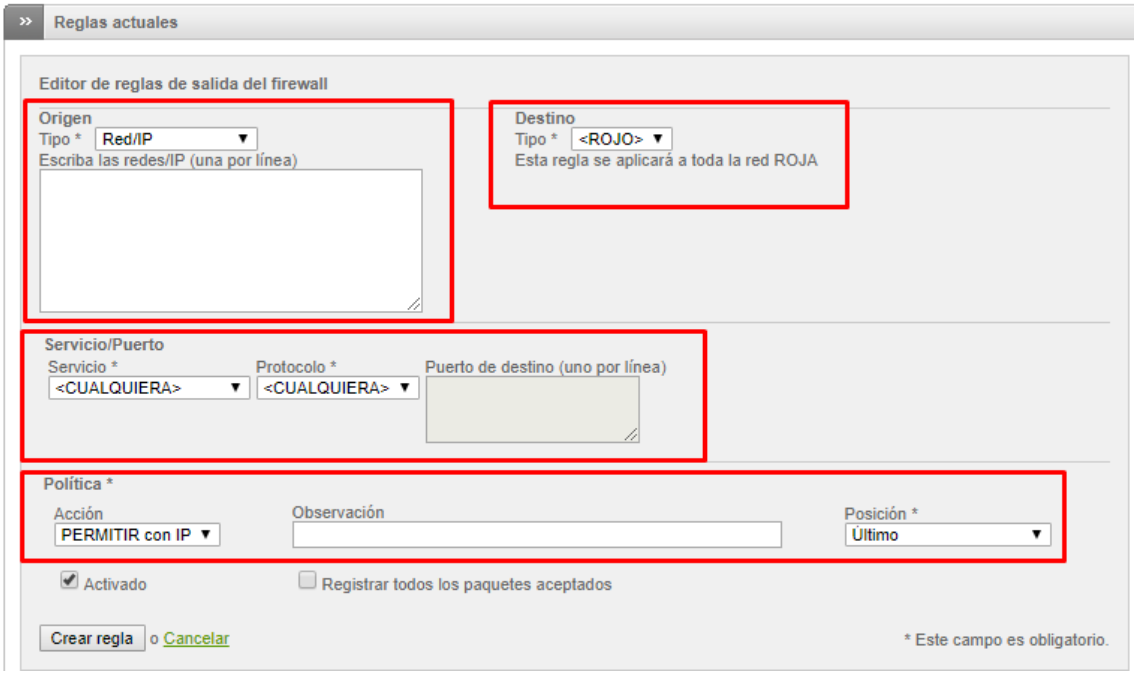


Figura 109. Configuración regla en firewall de salida
Fuente: Elaborado por el autor

Tráfico entre zonas: Con esta opción se puede aceptar o denegar los accesos entre las redes que administra el software Endian Firewall, como se puede observar en la figura 108 la presentación de cada una de las reglas está destinada a permitir el acceso a ciertos servicios y puertos de la DMZ ya que por defecto la política general es denegar todo.

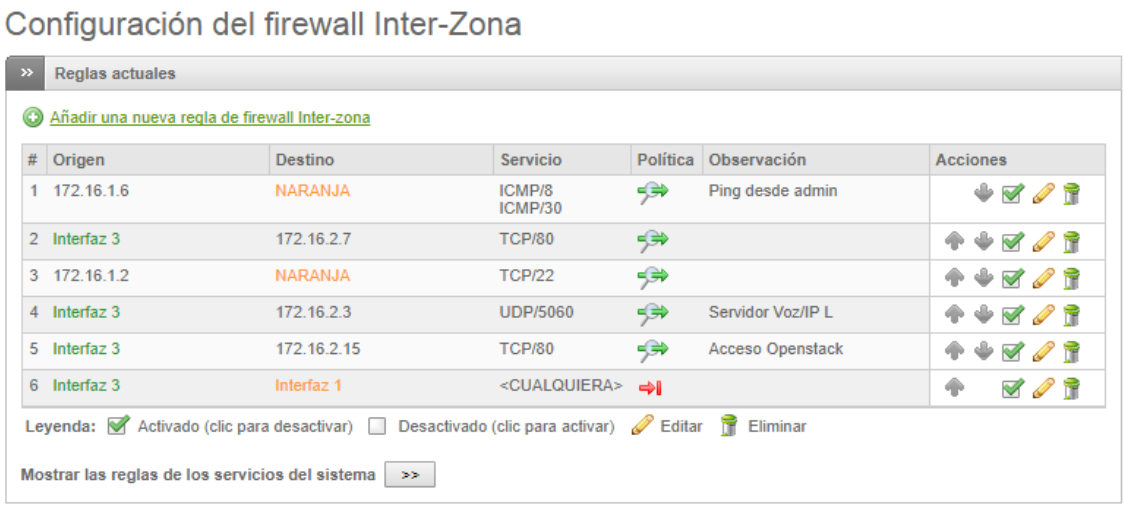


Figura 110. Reglas firewall inter-zona
Fuente: Elaborado por el autor

Acceso al sistema: dentro de este parámetro como se observa en la figura 109 se puede configurar tanto una dirección IP de acceso o una dirección MAC para que solo el administrador o un encargado temporal pueda acceder.

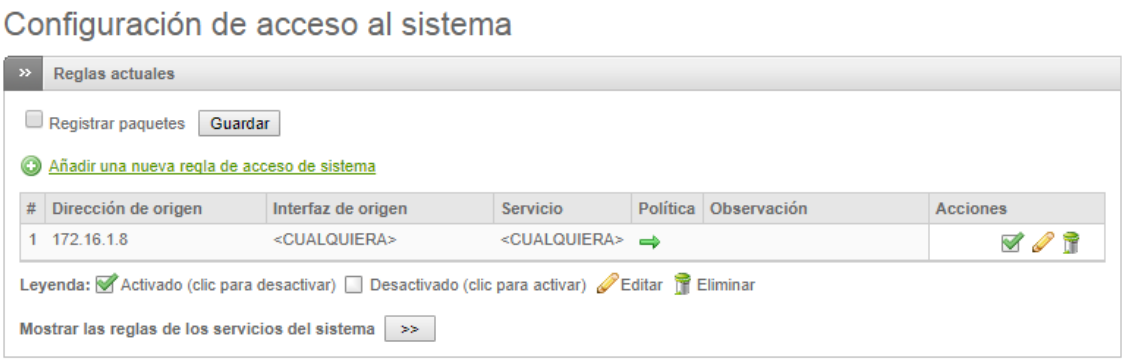


Figura 111. Configuración acceso al sistema
Fuente: Elaborado por el autor

Reportes e informes

Esta funcionalidad permite recopilar la información de cada uno de los servicios integrados en el software Endian firewall y los procesos de las herramientas y presentarlos de manera detallada por medio de un interfaz gráfico.

En la figura 110 se puede observar los servicios que se pueden visualizar como reportes en tiempo real.

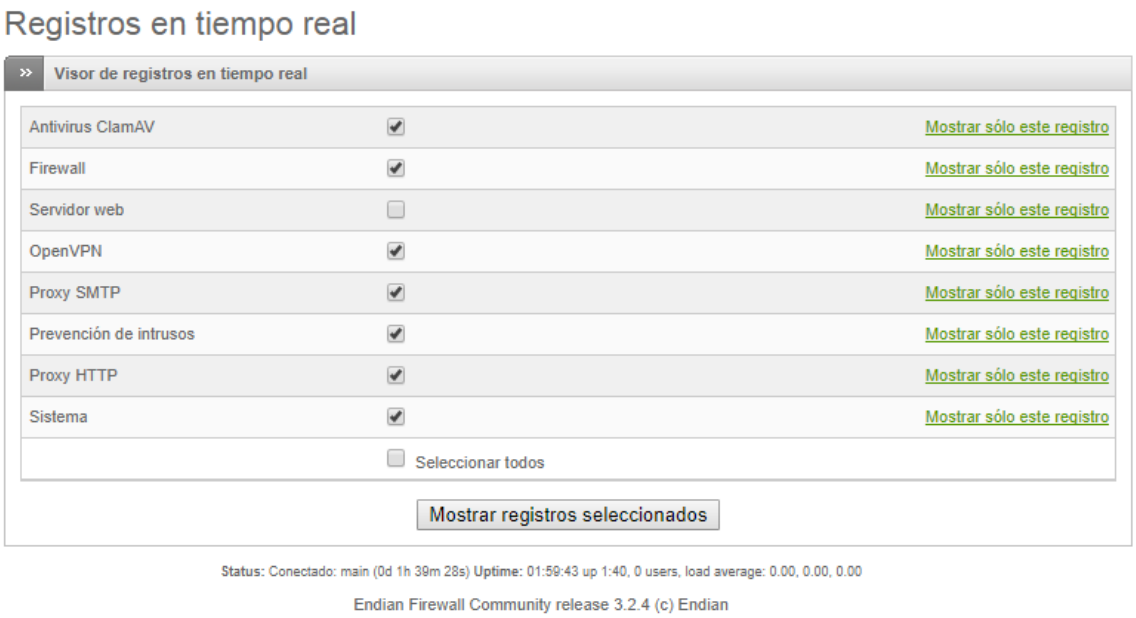


Figura 112. Panel de selección registros en tiempo real
Fuente: Elaborado por el autor

Para acceder se selecciona los casilleros del servicio que se desea visualizar y luego se da click sobre el botón de mostrar registros seleccionados, lo que despliega una ventana del navegador en la cual se puede observar en tiempo real los servicios cada uno identificado con un color que lo caracteriza para mejorar su interpretación y el proceso realizado como se observa en la Figura 111.

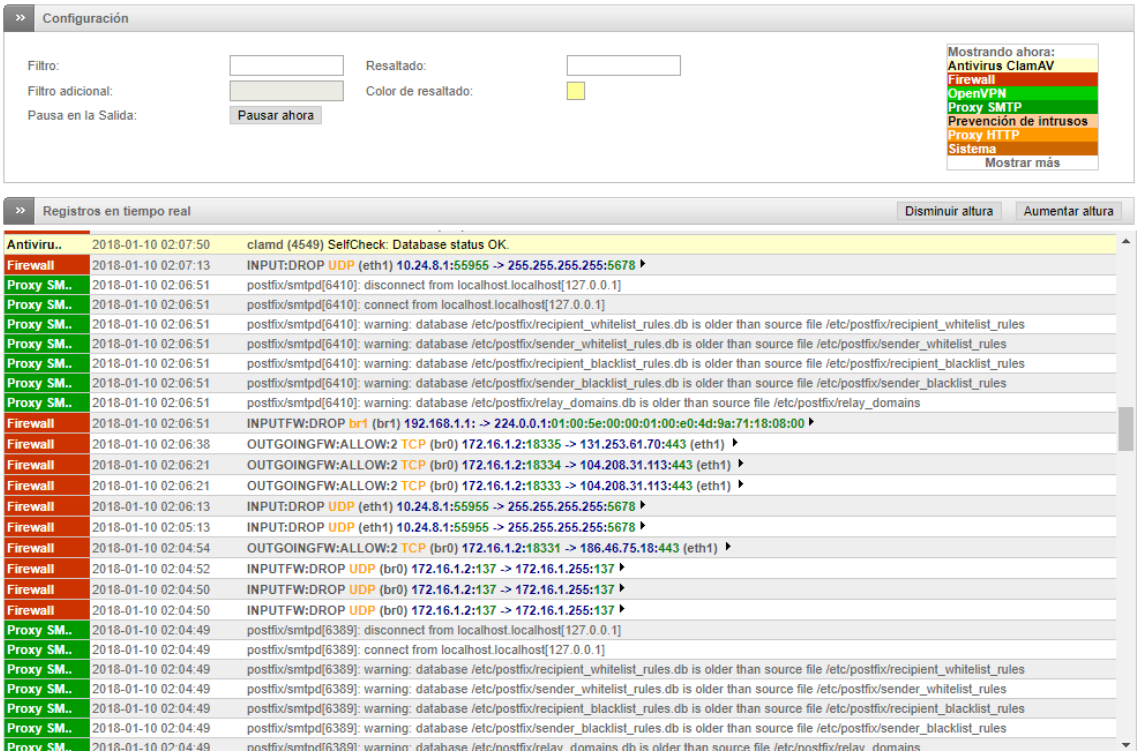


Figura 113. Reporte en tiempo real servicios Endian Firewall
Fuente: Elaborado por el autor

Además, se puede manejar etiquetas que permiten filtrar la búsqueda por medio de parámetros como IP, MAC, puerto o tipo de acceso.

Resumen del registro: Permite revisar por medio de fechas el informe resumido de la actividad del software y hardware donde se implementó Endian Firewall y además exportarlo en un archivo para presentación de reportes diarios. Este reporte se puede visualizar en la figura 112 y el archivo exportado del mismo en la figura 113.

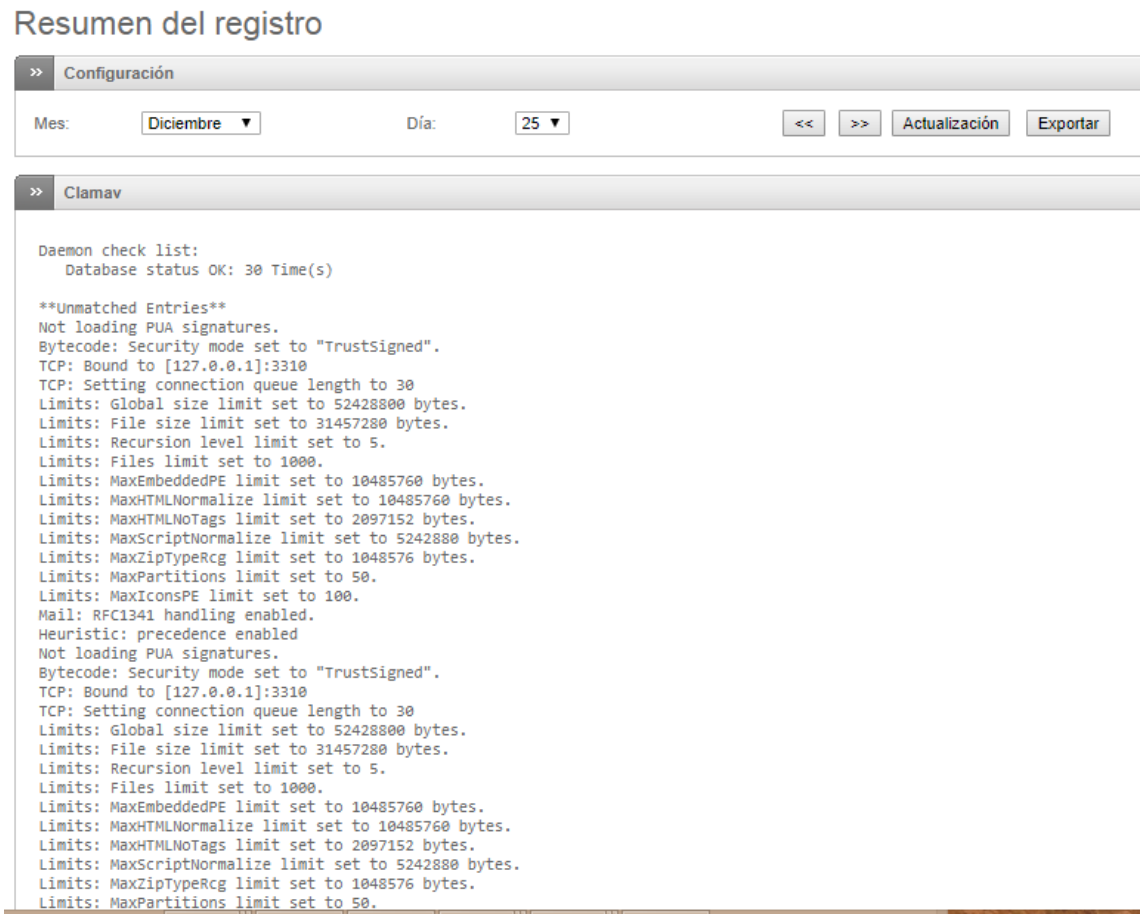


Figura 114. Reporte resumen de servicios activos diario
Fuente: Elaborado por el autor

```
################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Tue Dec 26 01:25:02 2017
        Date Range Processed: yesterday
                              ( 2017-Dec-25 )
                              Period is day.
      Detail Level of Output: 5
              Type of Output: unformatted
            Logfiles for Host: endian.localhost.com
 ##################################################################

--------------------- clam-update Begin ------------------------

No updates detected in the log for the freshclam daemon (the
ClamAV update process).  If the freshclam daemon is not running,
you may need to restart it.  Other options:

A. If you no longer wish to run freshclam, deleting the log file
   (default is freshclam.log) will suppress this error message.

B. If you use a different log file, update the appropriate
```

Figura 115. Reporte exportado
Fuente: Elaborado por el autor

Sistema: Permite revisar el reporte diario de las características y funcionamiento del sistema y los procesos que se habilitan constantemente o se dan de baja para encontrar fallos de inicialización o terminación de procesos como se observa en la figura 114 se puede seleccionar una fecha y permite exportarlo en un archivo que puede ser presentado como reporte de incidencias de forma diaria.

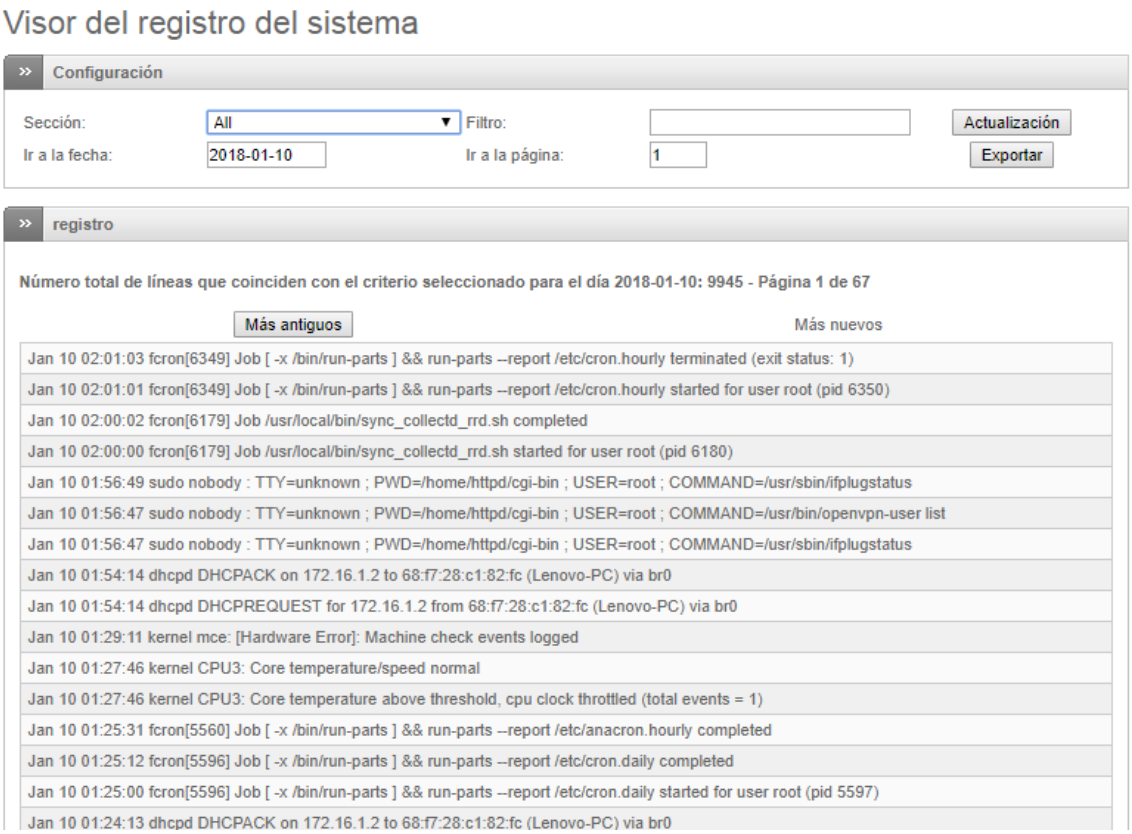


Figura 116. Reporte módulos activos sistema
Fuente: Elaborado por el autor

En la sección All se puede seleccionar varias opciones para delimitar la presentación del informe, de esta manera se permite independizar el reporte según servicios y aislar incidencias para posteriores análisis y auto aprendizaje de parte de quienes conforman el Data-Center.

Servicio: Este panel permite visualizar los reportes diarios de cada uno de los servicios que lo conforman que son IDS, OpenVPN y ClamAV los cuales se habilitan de ser requeridos por la organización, a su vez se pueden exportar y visualizar como se observa en la figura 115.

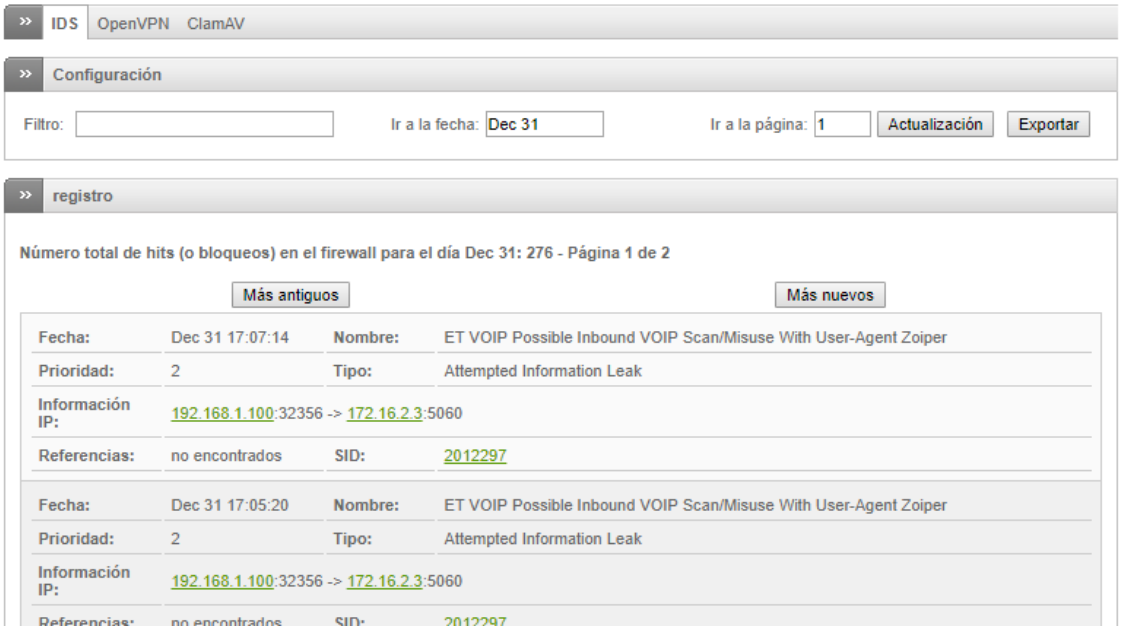


Figura 117. Visualización reporte de servicios de prevención
Fuente: Elaborado por el autor

Firewall: Permite visualizar y sacar reportes diarios de la actividad importante de rechazo o acceso según las políticas implementadas en el firewall como se observa en la figura 116, una vez seleccionado el día también permite exportar el reporte.

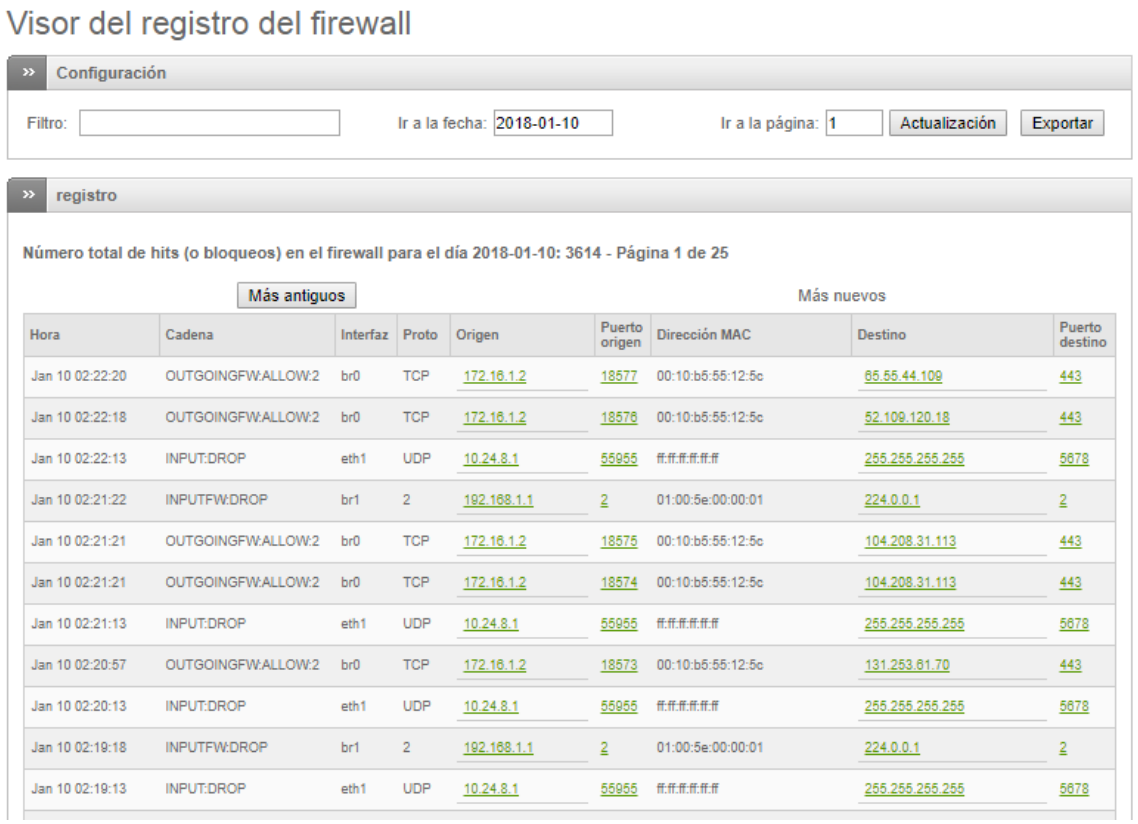


Figura 118. Visualización reporte de accesos y rechazos firewall
Fuente: Elaborado por el autor

Anexo 9: Criterios De Valorización

Escalas estándar

[pi] Información de carácter personal		
6	6.pi1	Probablemente afecte gravemente a un grupo de individuos
	6.pi2	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	Probablemente afecte gravemente a un individuo
	5.pi2	Probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	Probablemente afecte a un grupo de individuos
	4.pi2	Probablemente quebrante leyes o regulaciones
3	3.pi1	Probablemente afecte a un individuo
	3.pi2	Probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	Pudiera causar molestias a un individuo
	2.pi2	Pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	Pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	Probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	Probablemente sea un incumplimiento grave de una ley o regulación
3	3.lro	Probablemente sea un incumplimiento leve o técnico de una ley o regulación
1	1.lro	Pudiera causar el incumplimiento leve o técnico de una ley o regulación

[si] Seguridad		
10	10.si	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

9	9.si	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	Probablemente sea a causa de una merma en la seguridad o dificulte la investigación de incidentes graves
1	1.si	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o económicos		
9	9-cei-a	De enorme interés para la competencia
	9-cei-b	De muy elevado valor comercial
	9-cei-c	Causa de pérdida económica excepcionalmente elevadas
	9-cei-d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9-cei-e	Contribuye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei-a	De alto interés para la competencia
	7.cei-b	De elevado valor comercial
	7.cei-c	Causa de graves pérdidas económicas
	7.cei-d	Proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei-e	Contribuye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei-a	De cierto interés para la competencia
	3.cei-b	De cierto valor comercial

	3.cei-c	Causa de perdidas financieras o merma de ingresos
	3.cei-d	Facilitas ventajas desproporcionadas a individuos u organizaciones
	3.cei-e	Contribuye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei-a	De bajo interés para la competencia
	2.cei-b	De bajo valor comercial
1	1.cei-a	De pequeño interés para la competencia
	1.cei-b	De pequeño valor comercial
0	0.3	Supondría perdidas económicas mínimas

[da] Interrupción del servicio

9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la Interrupción de actividades propias de la Organización

[po] Orden público

9	9.po	Alteración sería del orden publico
6	6.po	Probablemente cause manifestaciones, o presiones significativas

3	3.po	Causa de protestas puntuales
1	1.po	Pudiera causar protestas puntuales

[olm] Operaciones

10	10.oml	Probablemente cause un daño excepcionalmente serio a la eficiencia o seguridad de la misión operativa o logística
9	9.oml	Probablemente cause daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.oml	Probablemente perjudique la eficiencia o seguridad de la misión operativa o logística
5	5.oml	Probablemente merme la eficiencia o seguridad de la misión operativa o logística
3	3.oml	Probablemente merme la eficiencia o seguridad de la misión operativa o logística (alcance local)
1	1.oml	Pudiera mermar la eficiencia o seguridad de la misión operativa o logística (alcance local)

[adm] Administración y gestión

9	9.adm	Probablemente impediría seriamente la operación efectiva de la Organización pudiendo llegar a su cierre
7	7.adm	Probablemente impediría la operación efectiva de la organización
5	5.adm	Probablemente impediría la operación efectiva de mas de una parte de la organización
3	3.adm	Probablemente impediría la operación efectiva de una parte de la organización
1	1.adm	Pudiera impedir la operación efectva de uan parte de la organización

[lg] Perdida de confianza(reputación)

9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones

	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente se causa una cierta publicidad negativamente a las relaciones con el publico
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una perdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una perdida menor de la confianza dentro de la Organización
0	0.lg	No supondría daño a la reputación o buena imagen de las personas u organizaciones

[crm] Persecución de delitos

8	8.crm	Impida la investigación de delitos graves o facilite u comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[rto] Tiempo de recuperación dl servicio

7	7.rto	RTO< 4 hora
4	4.rto	4 horas< RTO< 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)

10	10.lbl	Secreto

9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin Clasificar
1	1.lbl	Sin Clasificar

[lbl.ue] Información clasificada (Unión Europea)

10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONDIFENTIEL UE
7	7.ue	CONDIFENTIEL UE
6	6.ue	RETREINT UE
5	5.ue	RETREINT UE
4	4.ue	RETREINT UE
3	3.ue	RETREINT UE

Anexo 11: Matrices De Riesgo Situación Inicial

Matriz de riesgos para los activos con amenazas de origen natural e industrial

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]														
	Clasificación				Origen Natural			Origen Industrial											
Datos e Información	Disponibilidad	Integridad	Confidencialidad	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Fuego	Daños por agua	Desastres Naturales	Fuego	Daños por agua	Desastres industriales	Contaminación mecánica	Contaminación electromagnética	Avería Fisca/Lógica	Corte eléctrico	Condiciones inadecuadas	Fallo servicios comunicación	Interrupción servicios	Degradación soportes almacenamiento	Emanaciones electromagnéticas
					2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
IBM Systemx3200 M2 (Radius)	4	3	2	3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
HP Proliant DL360 G9 (Openstack)	3	4	4	4	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
HP Proliant ML150 G5 (Opina)	4	4	4	4	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
IBM Systemx3500 M4 (Reactivos 6 moodle)	4	4	4	4	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
IBM Systemx3500 M4 (DSpace)	3	3	3	3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
PC tipo Clon H8M-S1 (Biométricos)	4	3	3	3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
Switch de Core Catalyst 4506-E	4	2	3	3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
RouterBoard 1100 Mikrotik	4	2	2	3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
Switch de Distribución 3Com	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Switch de Distribución Linsys	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Switch Distribución inalámbrica QPCOM	3	1	1	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Figura 119. Matriz de riesgos con amenazas de origen natural e industrial
Fuente: Elaborada por el autor

Matriz de riesgos para los activos con amenazas de origen humano accidental o deliberado

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																														
	Clasificación				Origen Humano (Accidental)																Origen Humano (Deliberado)														
Datos e Información	Disponibilidad	Integridad	Confidencialidad	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Errores de los usuarios	Errores del administrador	Errores de monitorización	Errores de configuración	Difusión de software dañino	Errores de encaminamiento	Errores de secuencia	Escapes de información	Alteración accidental de la información	Destrucción de la información	Fugas de información	Vulnerabilidades de los programas	Errores de mantenimiento/actualiza	Errores de mantenimiento/actualiza	Caída del sistema por agotamiento de recursos	Pérdida de equipos	Manipulación de la configuración	Suplantación de la identidad del usuario	Abuso de privilegios de acceso	Uso no previsto	Difusión de software dañino	Re-encaminamiento de mensajes	Alteración de secuencia	Acceso no autorizado	Repudio	Modificación deliberada de la información	Destrucción de la información	Divulgación de información	Manipulación de programas	Manipulación de los equipos	Denegación de servicio	Robo	Ataque destructivo
					4	4	3	3	3	3	3	3	4	3	3	3	4	2	2	3	3	3	4	4	3	3	3	4	4	4	2	3	3	3	4	3	3
IBM Systemx3200 M2 (Radius)	4	3	2	3	12	12	9	9	9	9	9	9	12	9	9	9	12	6	6	9	9	9	12	12	9	9	9	12	12	12	6	9	9	9	12	9	9
HP Proliant DL360 G9 (Openstack)	3	4	4	4	16	16	12	12	12	12	12	12	16	12	12	12	16	8	8	12	12	12	16	16	12	12	12	16	16	16	8	12	12	12	16	12	12
HP Proliant ML150 G5 (Opina)	4	4	4	4	16	16	12	12	12	12	12	12	16	12	12	12	16	8	8	12	12	12	16	16	12	12	12	16	16	16	8	12	12	12	16	12	12
IBM Systemx3500 M4 (Reactivos 6 moodle)	4	4	4	4	16	16	12	12	12	12	12	12	16	12	12	12	16	8	8	12	12	12	16	16	12	12	12	16	16	16	8	12	12	12	16	12	12
IBM Systemx3500 M4 (DSpace)	3	3	3	3	12	12	9	9	9	9	9	9	12	9	9	9	12	6	6	9	9	9	12	12	9	9	9	12	12	12	6	9	9	9	12	9	9
PC tipo Clon H8M-S1 (Biométricos)	4	3	3	3	12	12	9	9	9	9	9	9	12	9	9	9	12	6	6	9	9	9	12	12	9	9	9	12	12	12	6	9	9	9	12	9	9
Switch de Core Catalyst 4506-E	4	2	3	3	12	12	9	9	9	9	9	9	12	9	9	9	12	6	6	9	9	9	12	12	9	9	9	12	12	12	6	9	9	9	12	9	9
RouterBoard 1100 Mikrotik	4	2	2	3	12	12	9	9	9	9	9	9	12	9	9	9	12	6	6	9	9	9	12	12	9	9	9	12	12	12	6	9	9	9	12	9	9
Switch de Distribución 3Com	2	1	1	1	4	4	3	3	3	3	3	3	4	3	3	3	4	2	2	3	3	3	4	4	3	3	3	4	4	4	2	3	3	3	4	3	3
Switch de Distribución Linsys	2	1	1	1	4	4	3	3	3	3	3	3	4	3	3	3	4	2	2	3	3	3	4	4	3	3	3	4	4	4	2	3	3	3	4	3	3
Switch Distribución inalámbrica QPCOM	3	1	1	2	8	8	6	6	6	6	6	6	8	6	6	6	8	4	4	6	6	6	8	8	6	6	6	8	8	8	4	6	6	6	8	6	6

Figura 120. Matriz de riesgos con amenazas de origen humano accidental o deliberado
Fuente: Elaborada por el autor

Anexo 12: Políticas Generadas En El Data-Center

UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS		
MANUAL DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION PARA EL DATACENTER		
	Versión	1.0.1
	Realizado por:	Sr. Cristian Alfonso Perugachi Msc. Carlos Vasquez
	Aprobado por:	

I.PROPOSITO

En el marco de normativa de seguridad es indispensable la adopción de políticas y procedimientos para el control de la seguridad de la información y el cumplimiento por parte de los encargados y usuarios que tengan relación con el centro de datos de la facultad de ingeniería y ciencias aplicadas, ubicado en la universidad técnica del norte de la ciudad de Ibarra, a su vez es necesario para resguardar el valor de los datos que maneja y los activos que los manipulan en su transmisión recepción procesamiento y almacenamiento.

II.GENERALIDADES

a. El documento detalla las políticas referentes a resguardar la seguridad lógica de los servicios y servidores que integran el Data-Center.

b. Este documento detalla las responsabilidades tanto de las personas encargadas del Data-Center así como los usuarios que interactúan con su infraestructura.

c. La persona tanto privada como particular que requiera acceso para mantenimiento, instalación o remoción de algún activo del centro de datos deberá conocer

el documento presente y actuar de acuerdo a la misma en caso de afectación se prevé tomar los correctivos adecuados establecidos.

III.VIGENCIA

El presente documento entrará en vigencia en el momento de su aprobación por las personas encargadas de la administración del centro de datos de la Facultad de Ingeniería y Ciencias Aplicadas, la misma que será revisada y actualizada conforme a las leyes o normativas actuales.

IV.REFERENCIA

Para su desarrollo se tomara en referencia la norma ISO/IEC 27002, la cual se encuentran desarrollados en forma de politicas los objetivos de control y controles presentados en el Anexo A de la norma ISO/IEC 27001, de los cuales se tomaran en cuenta los siguientes que abarcan la parte lógica de la red actual del Data-Center.

1. **Política de Seguridad de la Información**
    - 1.1. Documento de políticas de seguridad de la información.
    - 1.2. Revisión de las políticas de seguridad de la información.
2. **Organización de seguridad de la información**
    - 2.1. Compromiso de gestión de seguridad de la información.
    - 2.2. Coordinación de seguridad de la información
    - 2.3. Asignación de responsabilidades de seguridad de la información
    - 2.4. Proceso de autorización para instalaciones de procesamiento de información
    - 2.5. Contacto con las autoridades
    - 2.6. Contacto con grupos especiales de interés
    - 2.7. Revisión independiente de la seguridad de la información
3. **Gestión de los Activos**

3.1. Responsabilidad sobre los activos

3.2. Clasificación de la información

4. Gestión de Comunicaciones y Operaciones

4.1. Responsabilidades y procedimientos operacionales.

4.2. Aceptación y planificación del sistema

4.3. Protección contra código malicioso y descargable.

4.4. Respaldo de la información

4.5. Gestión de la seguridad de Red

4.6. Manipulación de dispositivos de almacenamiento externo

5. Control de Acceso

5.1. Gestión de acceso de usuario

5.2. Responsabilidades del usuario

5.3. Control de acceso a la red

5.4. Control de acceso al sistema operativo

5.5. Control de acceso a la información y aplicaciones

6. Gestión de incidentes en la seguridad de la información

6.1. Gestión de incidentes en la seguridad de la información

7. Cumplimiento

7.1. Cumplimiento de las políticas y normas de seguridad

V.TERMINOS Y DEFINICIONES

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
Acreditación	Acción de facultar a un sistema o red de información para que procese da- tos sensibles, determinando el grado en el que el diseño y la materializa- ción de dicho sistema cumple los requerimientos de seguridad técnica preestablecidos. [CESID:1997]
Activo	Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit: 2006]

Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]
Análisis de impacto	Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización.
Análisis de riesgos	Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
Ataque	Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006] Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID:1997]
Auditoría de seguridad	Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008] Aseguramiento de la identidad u origen. [Magerit:2006]
Certificación	Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [UNE 71504:2008] Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. [Magerit:2006] Característica que previene contra la divulgación no autorizada de activos del dominio. [Magerit:1997]
Declaración de aplicabilidad	Documento formal en el que, para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
Degradación	Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
Dimensión de seguridad	Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [UNE 71504:2008] Característica que previene contra la denegación no autorizada de acceso a activos del dominio. [Magerit:1997]

Estado de riesgo	Informe: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.
Evaluación de salvaguardas	Informe: Evaluación de la eficacia de las salvaguardas existentes en rela- ción al riesgo que afrontan.
Frecuencia	Tasa de ocurrencia de una amenaza. Número de sucesos o de efectos en una unidad de tiempo ISO Guía 73:2010]
Gestión de riesgos	Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [Magerit:2006] Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos. [Magerit:1997]
Impacto	Consecuencia que sobre un activo tiene la materialización de una amenaza. Consecuencia – Resultado de un suceso que afecta a los objetivos. [UNE- ISO Guía 73:2010]
Impacto residual	Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.
Incidente de seguridad	Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE 71504:2008] Evento con consecuencias en detrimento de la seguridad del sistema de información. [Magerit:2006]
Informe de insuficiencias	Informe: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir el riesgo sobre el sistema.
Integridad	Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008]
Mapa de riesgos	Informe: Relación de las amenazas a que están expuestos los activos.
Medida de seguridad	Véase salvaguarda.
Modelo de valor	Informe: Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.
Plan de seguridad	Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.
Probabilidad	Posibilidad de que un hecho se produzca. [UNE-ISO Guía 73:2010]
Proyecto de seguridad	Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.

Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
Riesgo acumulado	Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.
Riesgo potencial	Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes. [UNE 71504:2008]
Riesgo repercutido	Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.
Riesgo residual	Riesgo remanente en el sistema después del tratamiento del riesgo. [UNE- ISO Guía 73:2010] Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006] Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real. [Magerit:1997]
Salvaguarda	Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo. [UNE-ISO Guía 73:2010]
Seguridad	La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. [Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información].
Seguridad de la información	Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE 71504:2008]
Sistema de información	Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008] Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997] Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. [CESID:1997]

Tratamiento de riesgos	Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010]
Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008]
Valor	De un activo. Es una estimación del coste inducido por la materialización de una amenaza. Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE]
Valor acumulado	Considera tanto el valor propio de un activo como el valor de los activos que dependen de él. Bienes de abolengo: Los heredados de los abuelos. [DRAE]
Vulnerabilidad	Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.

VI.DESARROLLO DE POLITICAS DE SEGURIDAD

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	1. Políticas de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	1.1. Documento de políticas de seguridad de la información	**Fecha de Elaboración:**	

Art. 1. Proporcionar las directrices de la dirección y el soporte para la seguridad de la información en acuerdo con los requerimientos de la FICA, de esta manera proteger los activos que conforman el Data-Center tanto hardware como software en base al estándar ISO 27001.

a) Las políticas deben presentarse a toda la organización que conforma el centro de datos FICA de manera comprensible al lector, se puede anexar a un documento general de políticas de la organización.
b) En caso de distribución externa se debe resguardar la información confidencial de las políticas.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	1. Políticas de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	1.2. Revisión de las políticas de la seguridad de la información	**Fecha de Elaboración:**	

Art. 2. Los administradores de la seguridad del Data-Center deben revisar las políticas de la seguridad de información en intervalos planificados además en caso de realizarse cambios significativos para asegurar su actualización, idoneidad y continuidad.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.1. Compromiso de gestión de seguridad de la información	**Fecha de Elaboración:**	

Art. 3. La administración apoyara activamente la seguridad de la información dentro del Data-Center por medio de políticas claras, compromiso adecuado y asignación clara de responsabilidades.

Las responsabilidades de la administración son:

a) Identificar los objetivos de seguridad de la información
b) Revisar las políticas de la información y su aprobación.
c) Proporcionar un apoyo permanente en los proyectos de seguridad de la información
d) Proporcionar los recursos necesarios
e) Aprobar la asignación de funciones y responsabilidades de las personas relacionadas con el Data-Center.

f) Socializar los planes de seguridad de la información

Art. 4. La administración debe identificar las necesidades de asesoramiento especializado interno o externo, además de su documentación.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.2. Coordinación de seguridad de la información	**Fecha de Elaboración:**	

Art. 5. Los administradores del Data-Center FICA deben implicar la coordinación y colaboración de los usuarios, diseñadores de aplicaciones, auditores, personal de seguridad, personal administrativo y docente, de esta manera asignar sus roles y responsabilidades.

a) Identificar penalizaciones por exceder los roles o funciones asignadas.
b) Establecer los procesos para la seguridad de la información.
c) Identificar los cambios significativos en el Data-Center.
d) Promover la formación en materia de seguridad de la información.

Art. 6. Las responsabilidades y tareas asignadas no podrán ser excedidas para de esta manera evitar modificaciones no autorizadas o el mal uso de los activos del Data-Center de la FICA.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.3. Asignación de responsabilidades de seguridad de la información	**Fecha de Elaboración:**	

Art. 7. La administración realizara la asignación de responsabilidades en acuerdo con las políticas de la información.

Art. 8. Las áreas de responsabilidad deben estar claramente definidas y se debe realizar lo siguiente:

a) Los activos y procesos de seguridad deben estar claramente definidos
b) Se debe asignar responsabilidades particulares según el activo y el proceso.
c) Los niveles de autorización deben ser definidos y documentados.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.4. Proceso de autorización para instalaciones de procesamiento de información	**Fecha de Elaboración:**	

Art. 9. Se debe tomar en cuenta las siguientes indicaciones para la autorización de procesos:

a) Instalaciones nuevas deben tener previa autorización del administrador de la red, junto con un documento que indique su propósito y el cumplimiento de las políticas de seguridad de la información.
b) Verificar la compatibilidad del hardware y software con el sistema a implementar
c) La utilización de equipos externos para la configuración o mantenimiento de los activos dentro del Data-Center.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.5. Contacto con las autoridades	**Fecha de Elaboración:**	

Art. 10. Los administradores del Data-Center deben tener el contacto adecuado con las autoridades superiores de la Universidad Técnica del Norte para informar de cualquier incidente en la seguridad de la información que afecte al funcionamiento de los servicios implementados.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.6. Contacto con grupos especiales de interés	**Fecha de Elaboración:**	

Art. 11. Los administradores del Data-Center tienen que mantener contactos adecuados con grupos de interés especial, foros de seguridad y grupos profesionales.

Art. 12. El mantener el contacto con grupos de interés presenta las siguientes ventajas:

a) Mejores prácticas y actualización permanente en la seguridad de la información.
b) Recibir alertas tempranas antes amenazas y vulnerabilidades.
c) Acceso a asesoría especializada.
d) Compartir e intercambiar información.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	2. Organizaciones de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	2.7. Revisión independiente de la seguridad de la información	**Fecha de Elaboración:**	

Art. 13. Los administradores deben implementar una revisión independiente en intervalos planificados para revisión de cambios significativos en la seguridad de la información.

Art. 14. La revisión debería ser llevada por personal independiente del área cercana al Data-Center de la FICA, con habilidades y experiencia relacionada con el área de seguridad del a información.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	3. Gestión de activos	**Destinatarios:**	Todos los usuarios
	Control:	3.1. Responsabilidad de activos	**Fecha de Elaboración:**	

Art. 15. Los administradores se encargarán de que los activos sean identificados, tengan un propietario, estén asignadas sus funciones, e integren controles apropiados.

Art. 16. Los administradores del Data-Center de la FICA deben encargarse de tener claramente identificados los activos.

Existen varios tipos de activos los cuales son:

a) Información: bases de datos y archivos, acuerdos, documentación de sistemas, investigaciones, manuales de usuario, procedimientos de soporte, planes de continuidad, información archivada, etc.

b) Activos de Software: aplicaciones, sistemas y herramientas de desarrollo.

c) Activos Físicos: equipos de computación, equipos de comunicación, dispositivos portátiles y otros equipos.

d) Servicios: Servicios de comunicación y computación.

Art. 17. Toda la información de los activos y su procesamiento debe ser asignado a un propietario que sea parte de la FICA

El propietario del activo es responsable por:

a) Asegurarse de que la información del activo sea procesada y clasificada de manera apropiada.

b) Definir un periodo para la revisión de permisos de acceso.

Art. 18. El administrador del Data-Center FICA y el propietario del activo deben definir las reglas y la documentación pertinente para su uso.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	3. Gestión de activos	**Destinatarios:**	Todos los usuarios
	Control:	3.2. Clasificación de la información	**Fecha de Elaboración:**	

Art. 19. La información debe clasificarse para indicar la necesidad, las prioridades y su grado de protección.

Art. 20. Las clasificaciones y los controles de protección deben tomar en cuenta las necesidades del usuario final del Data-Center FICA.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.1. Responsabilidades y procedimientos operacionales	**Fecha de Elaboración:**	

Art. 21. Los administradores tienen la tarea de establecer responsabilidades y procedimientos para la gestión de todos los activos encargados del procesamiento de información.

Art. 22. Se deberán establecer los procedimientos de inicio, terminación, respaldo, mantenimiento del equipo.

Estos procedimientos deben contar con los siguientes parámetros:

a) Tratamiento de la información
b) Tiempos de realización de un trabajo
c) Contacto de apoyo técnico
d) Instrucciones especiales para el manejo del activo
e) Procedimiento de reinicio y recuperación del sistema
f) Gestión de la información de registro.

Art. 23. Los cambios en los sistemas de procesamiento de la información deben ser controlados.

Los siguientes parámetros deben ser considerados en particular:

a) Identificación de cambios significativos.
b) Planificación y comprobación de cambios.
c) Evaluación de posibles impactos
d) Aprobación de cambios propuestos.

Art. 24. Se debe separar las funciones y responsabilidades para reducir las posibilidades de cambios no autorizados o mala utilización de los activos del Data-Center FICA.

En una organización pequeña como se puede considerar al Data-Center FICA se lo aplicara en la medida de lo posible.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.2. Aceptación y planificación del sistema	**Fecha de Elaboración:**	

Art. 25. Los administradores deben planificar de manera anticipada los recursos necesarios del sistema que se implementara para evitar sobrecargas que incidan en el funcionamiento de los servicios integrados en el Data-Center FICA.

Art. 26. Los administradores del Data-Center FICA tienen que identificar las condiciones de los recursos del sistema mediante un sistema de monitorización para identificar posibles cuellos de botella y tomar las medidas adecuadas para evitar pérdidas de información.

Art. 27. Los administradores del Data-Center FICA tienen que asegurar que se cumplan los requisitos de adaptación para la implementación de sistemas y actualizaciones.

Para poder integrar un sistema es necesario cumplir con lo siguiente:

a) Requerimientos de sistema
b) Procedimiento de recuperación, reinicio y planes de contingencia.
c) Procedimientos manuales
d) Pruebas de funcionamiento

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.3. Protección contra código malicioso y descargable.	**Fecha de Elaboración:**	

Art. 28. Se debe tener en cuenta las precauciones para prevenir y detectar la introducción de código malicioso.

Art. 29. Los administradores deben implementar los controles de detecccion, prevención y recuperación para proteger contra código malicioso.

Se debe implementar un software de detección de código malicioso para el cual se debe considerar lo siguiente:

a) Evitar uso no autorizado de software en los activos que integran el Data-Center
b) Realizar revisiones periódicas de los activos que manejan información sensible de la organización.
c) Instalación y actualización de software de detección de código malicioso.
d) Comprobación de cualquier medio extraíble que ingrese al Data-Center
e) Definir procedimientos para enfrentar una infección
f) Preparación de planes de continuidad

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.4. Respaldo de la información	**Fecha de Elaboración:**	

Art. 30. Los administradores del Data-Center FICA establecerán los procedimientos de rutina y la estrategia de respaldo de la información.

Art. 31. Se debe realizar instalaciones de respaldo de la información importante y el software en caso de existir un desastre o fallo generalizado

Hay que considerar lo siguiente para la información de respaldo:

a) Registro de la información de respaldo y los procedimientos a realizar para su restauración
b) La frecuencia de realización de respaldos de estar documentada
c) Las copias de seguridad deben almacenarse en una ubicación externa.
d) Se debe probar periódicamente la información de respaldo
e) Los respaldos pueden ser protegidos mediante cifrado

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.5. Gestión de la seguridad de red	**Fecha de Elaboración:**	

Art. 32. Los administradores de la red deben proteger la información mediante sistemas de seguridad aplicados en la infraestructura de red.

Art. 33. Las redes deben estar gestionadas y controladas para protegerlas de amenazas externas e internas que ponen en riesgo la seguridad de los sistemas, para esto los administradores del Data-Center FICA deben considerar lo siguiente:

a) Deben establecerse responsabilidades y procedimientos para la gestión de equipos remotos.
b) Se deben establecer controles especiales para proteger la confidencialidad e integridad de los datos que se transportan por redes públicas e inalámbricas.
c) Se debe implementar el monitoreo en la red para registrar acciones relevantes de seguridad.

Art. 34. Se debe implementar controles de seguridad que le den un valor agregado como separación de redes privadas, implementación de un firewall y sistema de detección de intrusiones.

Las características a tomar en cuenta son las siguientes:

a) Autenticación, cifrado y controles de conexión a red.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	4. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	4.6. Manipulación de dispositivos de almacenamiento externo	**Fecha de Elaboración:**	

Art. 35. Los administradores del Data-Center FICA deben establecer los procedimientos para la entrada o salida de medios externos.

Art. 36. Se debe tomar en cuenta las siguientes directrices para el manejo de medios externos:

a) Si el contenido del medio extraíble ya no es necesario se debe destruir la información que contenga.
b) Se debe requerir autorización para la utilización de los medios extraíbles removidos del Data-Center FICA.
c) Todos los medios extraíbles deben almacenarse en un entorno seguro.
d) Se debe registrar los medios extraíbles que ingresan o salen del Data-Center.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	5.1. Gestión de acceso de usuario	**Fecha de Elaboración:**	

Art. 37. Los administradores del Data-Center FICA deben generar los procedimientos para todos los ciclos de vida de acceso de usuario desde el registro inicial de nuevos usuarios hasta su eliminación, además de contar con un control que permita asignar Se deberán tomar en cuenta los niveles de acceso establecidos según el usuario.

Art. 38. El procedimiento para el registro y cancelación de acceso para cada usuario debe incluir:

a) Usar identificadores únicos para asignar responsabilidades directas al usuario.
b) Autorización del propietario del sistema o servicio de información.
c) Nivel de acceso concedido.
d) Declaración escrita de sus derechos de acceso.
e) Firma de responsabilidad del usuario
f) Registro formal de las personas autorizadas.
g) Eliminar el acceso a los usuarios que finalizaron su trabajo en el Data-Center FICA
h) Revisar periódicamente los derechos de acceso.

Art. 39. Los sistemas que requieran protección contra accesos no autorizados deben tener un control basado en un proceso formal de autorización, que contempla los siguientes pasos:

a) Los privilegios de acceso según el sistema y las aplicaciones.
b) Privilegios asignados según el evento que se presento
c) Registro de todos los privilegios asignados según el usuario
d) Se debe asignar un ID independiente por usuario.

Art. 40. La asignación de contraseñas para el acceso a los sistemas u servicios debe incluir los siguientes requisitos:

a) Firma de responsabilidad del usuario.
b) En caso de que todos los usuarios requieran una contraseña para el uso de un servicio se les asignara una temporal, que deberán cambiar inmediatamente por una de su preferencia.
c) Establecer los procedimientos para verificar la identidad de un usuario antes de restablecer una contraseña.
d) Las contraseñas temporales deben entregarse a los usuarios de manera segura.
e) Las contraseñas deben almacenarse en sistemas con las seguridades necesarias.

f) Se debe reemplazar las contraseñas predeterminadas de un sistema después de su instalación.

Art. 41. Los administradores del Data-Center FICA deben revisar los derechos de acceso a los usuarios en intervalos regulares, tomando en cuenta los siguientes parámetros:

a) Los derechos de acceso de usuario deben revisarse cada 6 meses y después de cualquier cambio en los privilegios o posición del usuario.
b) Los derechos deben ser revisados y reasignados cuando un usuario cambia de posición laboral dentro de la Universidad Técnica del Norte.
c) Los accesos con privilegios especiales deben ser revisados cada 3 meses.
d) Los cambios en accesos privilegiados deben registrarse de manera mensual.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	5.2. Responsabilidades del usuario	**Fecha de Elaboración:**	

Art. 42. Los usuarios deben ser conscientes de sus responsabilidades en lo que se refiere a uso de contraseñas y seguridad de su equipo de trabajo.

Art. 43. Los usuarios deben realizar buenas prácticas de seguridad en la selección y uso de las contraseñas, por medio de los siguientes pasos:

a) Mantener la confidencialidad de las contraseñas
b) No almacenar la contraseña en un registro de fácil acceso.
c) Cambiar la contraseña en caso de vulnerabilidades en el sistema
d) Contraseña con longitud aceptable:
    1. Fácil de recordar

2. No relacionada con aspectos directamente relacionados a la persona
3. No vulnerables a ataques de diccionario
4. Sin caracteres consecutivos o repetitivos.

e) Cambiar la contraseña en intervalos regulares

f) No almacenar las contraseñas en la cache de los navegadores

g) Cambiar contraseñas temporales en el primer inicio de sesión

h) No compartir contraseñas individuales de los usuarios.

i) No usar la misma contraseña en todas las cuentas.

Art. 44. El usuario debe estar consciente de los procedimientos y requisitos para proteger un equipo del Data-Center FICA, la recomendación general es:

a) Cerrar sesiones activas al terminar.

b) Asegurar los terminales mediante contraseña en caso de no utilizarlo.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	5.3. Control de acceso a la red	**Fecha de Elaboración:**	

Art. 45. Los administradores del Data-Center FICA regularan el acceso de los usuarios a las redes y servicios para no comprometer su seguridad y garantizar:

a) Interfaces apropiadas de comunicación entre la red del Data-Center FICA, las redes públicas y la intranet de la Universidad Técnica del Norte.

b) Mecanismos de autenticación entre los usuarios y el equipo.

c) Control de acceso del usuario a los servicios.

Art. 46. La política abarca lo siguiente:

a) Redes y servicios que se puede acceder

b) Procedimientos para la autorización a redes y servicios.

c) Protección de conexiones de red.

Art. 47. La autenticación de usuarios remotos con privilegios se realizará mediante controles criptográficos y la utilización de técnicas como VPN, o doble autenticación utilizando la dirección MAC.

Art. 48. Es recomendable dividir en dominios la red lógica, y separar la red pública de la intranet y la DMZ de los Data-Center, se puede aplicar un Gateway o firewall que se encargue de separar y proteger los sistemas y servicios.

Art. 49. Para todas las redes externas que soliciten acceso a los servicios de la organización se debe restringir a través de pasarelas, firewall o proxy de red que filtren el tráfico. Para aplicaciones como:

a) Correo electrónico

b) Transferencia de archivos

c) Acceso interactivo

d) Acceso a la aplicación

Art. 50. Las instalaciones de seguridad deben usarse para restringir el acceso a los sistemas operativos a los usuarios no autorizados, considerando que las instalaciones deben ser capaces de:

a) Autenticar usuarios no autorizados.

b) Registrar intentos de autenticación exitosos o fallidos.
c) Registrar el uso de privilegios especiales del sistema.
d) Emitir alarmas cuando se rompan las seguridades.
e) Proporcionar medios adecuados para la autenticación
f) Regular tiempos de conexión

Art. 51. Se deben establecer procedimientos para minimizar posibilidades no autorizados, para esto debe cumplir los siguientes requisitos:

a) No mostrar identificadores de sistema hasta que no se complete el inicio de sesión.
b) Advertencia general de que solo los usuarios autorizados deben tener acceso a la computadora
c) No mostrar mensajes de ayuda para inicio de sesión
d) Limitar número de intentos para autenticación y registrarlos
e) Registrar login exitoso
f) No mostrar la contraseña introducida.
g) No transmitir contraseñas en texto plano a través de una red

Art. 52. Los sistemas de contraseñas deben ser interactivos y deben garantizar contraseñas de calidad realizando lo siguiente:

a) Imponer el uso de identificadores de usuario y contraseñas individuales
b) Permitir al usuario seleccionar y cambiar su contraseña mediante confirmación
c) Imponer parámetros para la selección de contraseñas
d) Obligar al cambio de contraseña temporal en el primer inicio de sesión
e) Evitar reutilización de contraseñas
f) Almacenar las contraseñas de manera independiente
g) Almacenar y transmitir contraseñas de forma protegida

Art. 53. Los administradores deben integrar medidas de seguridad que permitan controlar los tiempos en pantalla de sesión, además de cierre de conexiones inactivas que exceden cierta cantidad de tiempo.

Art. 54. Los controles de conexión por tiempo deben ser implementados en aplicaciones informáticas sensibles y en conexiones desde una red pública.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	5. Control de accesos	**Destinatarios:**	Todos los usuarios
	Control:	5.5. Control de acceso a la información y aplicaciones	**Fecha de Elaboración:**	

Art. 55. El acceso lógico al software de la aplicación y la información debe limitarse a los usuarios autorizados.

Los sistemas de aplicación deben:

a) Proteger de accesos no autorizados y software malintencionado.
b) Aislar los sistemas en caso de una infección que comprometa recursos

Art. 56. Los administradores del Data-Center FICA deben implementar los siguientes requisitos de restricción:

a) Proporcionar menús para controlar las funciones del sistema.
b) Controlar permisos del usuario para lectura y escritura.
c) Asegurar la información sensible para su envió y compartición solo a servidores y usuarios autorizados.

Art. 57. Se debe tomar en cuenta las siguientes consideraciones para los sistemas informáticos sensibles:

a) El propietario del sistema debe documentar la sensibilidad del sistema.

b) El propietario debe identificar los sistemas con los que interactuara la información sensible contenida.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	6. Gestión de incidentes de seguridad de la información	**Destinatarios:**	Todos los usuarios
	Control:	6.1. Gestión de incidentes en la seguridad de la información	**Fecha de Elaboración:**	

Art. 58. Todo usuario y empleado que se relacione con el Data-Center FICA debe reportar cualquier tipo de evento o vulnerabilidad que incide directamente en la seguridad de los activos.

Art. 59. Se seguirá el procedimiento para presentación de informes sobre los sucesos de la seguridad de la información, además de respuesta y escalamiento de incidentes.

Estos procesos deberán incluir:

1. Retroalimentación para asegurar que no se repitan las mismas fallas.
2. Formularios de información de eventos.
3. Comportamiento correcto en caso de vulnerabilidades siguiendo el proceso descrito
   - 3.1. Anotar todos los detalles importantes
   - 3.2. Informar a los administradores del Data-Center FICA

Art. 60. Los documentos de resolución de incidentes deberán ser del conocimiento de todos los usuarios que accedan al Data-Center y de esta manera reducir la probabilidad de incidentes futuros.

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Dominio:	7. Cumplimiento	**Destinatarios:**	Todos los usuarios
	Control:	7.1. Cumplimiento de las políticas y normas de seguridad	**Fecha de Elaboración:**	

Art. 53. Los encargados del Data-Center FICA tienen la responsabilidad de verificar el cumplimiento de las políticas de seguridad.

Art. 54. Las sanciones que se pueden presentar por el incumplimiento de las políticas son las siguientes:

a) Llamado de atención de manera escrita y verbal

b) Suspensión temporal del acceso a los activos del Data-Center

c) Suspensión permanente del acceso a los activos del Data-Center

d) Reposición del costo de los activos dañados, sustraídos o extraviados que se den por acción directa del usuario o encargado.

Anexo 13: Formato Reporte De Incidencias

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

Reporte de incidencias de seguridad en el Data-Center

Datos Personales	
Nombre Completo:	CI:
Responsabilidad Asignada:	Firma:
Información sobre el incidente	
Fecha de detección:	Código del incidente:
Activo afectado (directamente):	Servicios afectados:
Activos afectados (Indirectamente):	Duración del incidente:
¿Cómo se detectó el incidente?	
Ubicación Física:	
Valoración del incidente	

Disponibilidad:

	Muy Bajo	No Aplica/No es relevante
	Bajo	Debe estar disponible al menos el 10%
	Medio	Debe estar disponible al menos el 50%
	Alto	Debe estar disponible al menos el 99%

Integridad:

	Muy Bajo	No Aplica/No es relevante
	Bajo	No es relevante los errores que tenga o la información que falte
	Medio	Tiene que estar correcto y completo al menos en un 50%
	Alto	Tiene que estar correcto y completo al menos en un 95%

Confidencialidad:

	Muy Bajo	No Aplica/No es relevante
	Bajo	Daños muy bajos, el incidente no trascendería del área afectada
	Medio	Serian relevantes, el incidente implicaría a otras áreas
	Alto	Los daños serian catastróficos, la reputación y la imagen de la organización se verían comprometidas

Anexo 14: Formato Procedimiento Realizado

	UNIVERSIDAD TÉCNICA DEL NORTE **FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS** **Procedimiento en un activo del Data-Center**

Datos Personales	
Nombre Completo:	CI:
Responsabilidad Asignada:	Firma:
Tipo de procedimiento: Desarrollo ☐ Prueba: ☐ Operacional: ☐	
Información del Activo o Activos (Antes de procedimiento)	
Identificador:	Encargado:
Función desempeñada o Servicio brindado:	Ubicación Física:
¿Descripción del procedimiento realizado?	
Fecha de realización:	Duración de la Actividad:
Observaciones/Resultados:	
Información del Activo (Después de procedimiento)	
Función desempeñada o Servicio brindado:	Ubicación Física:
Nota: Llenar esta sección solo si se modificó la configuración o función del activo en la red	

Anexo 15: Formato Eliminación De Activo O Medio Removible

	UNIVERSIDAD TÉCNICA DEL NORTE **FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS** **Formato eliminación de activo o medio removible**

Datos Personales	
Nombre Completo:	CI:
Responsabilidad Asignada:	Firma:

Información del activo				
No.	Descripción del activo	Identificador		Responsable
	Disco Duro	Funciona		Ubicación Física
	RAM	Si	No	
	Procesador	Si	No	
	Fuente	Si	No	
	Monitor	Si	No	
	Procesador	Si	No	
	Memoria extraíble	Si	No	
	Tarjeta de Red	Si	No	
	Tarjeta de Video	Si	No	

Observaciones

Firma Administrador del Data-Center
CI:

Anexo 16: Solicitud Para Procedimientos En El Data-Center

UNIVERSIDAD TÉCNICA DEL NORTE
Facultad de Ingeniería en Ciencias Aplicadas

SOLICITUD DE INGRESO AL CENTRO DE DATOS FICA

Fecha: *Fecha de Entrega de la solicitud*
Dirigido a: *Administrador responsable del Data-Center*
Solicitante: N*ombre(s) del solicitante*
Responsabilidad: *Ocupación que desempeña dentro del Data-Center*
Asunto: *Motivo de la solicitud*

MOTIVO DE LA SOLICITUD Y DESCRIPCIÓN
SOLICITUD DE ACCESO
SOLICITUD DE COMPRA DE UN ACTIVO
SOLICITUD DE MANTENIMIENTO
SOLICITUD DE INTEGRACION DE UN ACTIVO

Este documento puede detallar las características de los activos en caso de ser necesario y cronogramas

Atentamente,
FIRMA DEL/LOS SOLICITANTES
CI: XXXXXXXX X

Anexo 17: Manual de Procedimientos

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Procedimiento:	Solicitud de acceso al Data-Center	**Destinatarios:**	Todos los usuarios
	Identificador:	PR-1.0.1	**Fecha de Elaboración:**	

1. Objetivo: Habilitar el acceso al Data-Center a usuarios externos al entorno de administración tanto para revisión, instalación o remoción de equipos.
2. Alcance: Se aplica a los usuarios que soliciten acceso al Data-Center
3. Definiciones:
    - Data-Center: Es el centro de equipos donde se centraliza todos los recursos de la red, servidores, equipos de red, cableado estructurado, racks, sistema de enfriamiento.
    - Administrador de red: Persona encargada del Data-Center, mejor conocido como jefe de TICs.
    - Usuario solicitante: Persona particular que tiene relación directa o indirecta con la universidad técnica del norte entre los cuales se pueden encontrar personal docente, administrativo o estudiantil.
    - TICs: Tecnologías de información y comunicación.

Diagrama de Flujo:

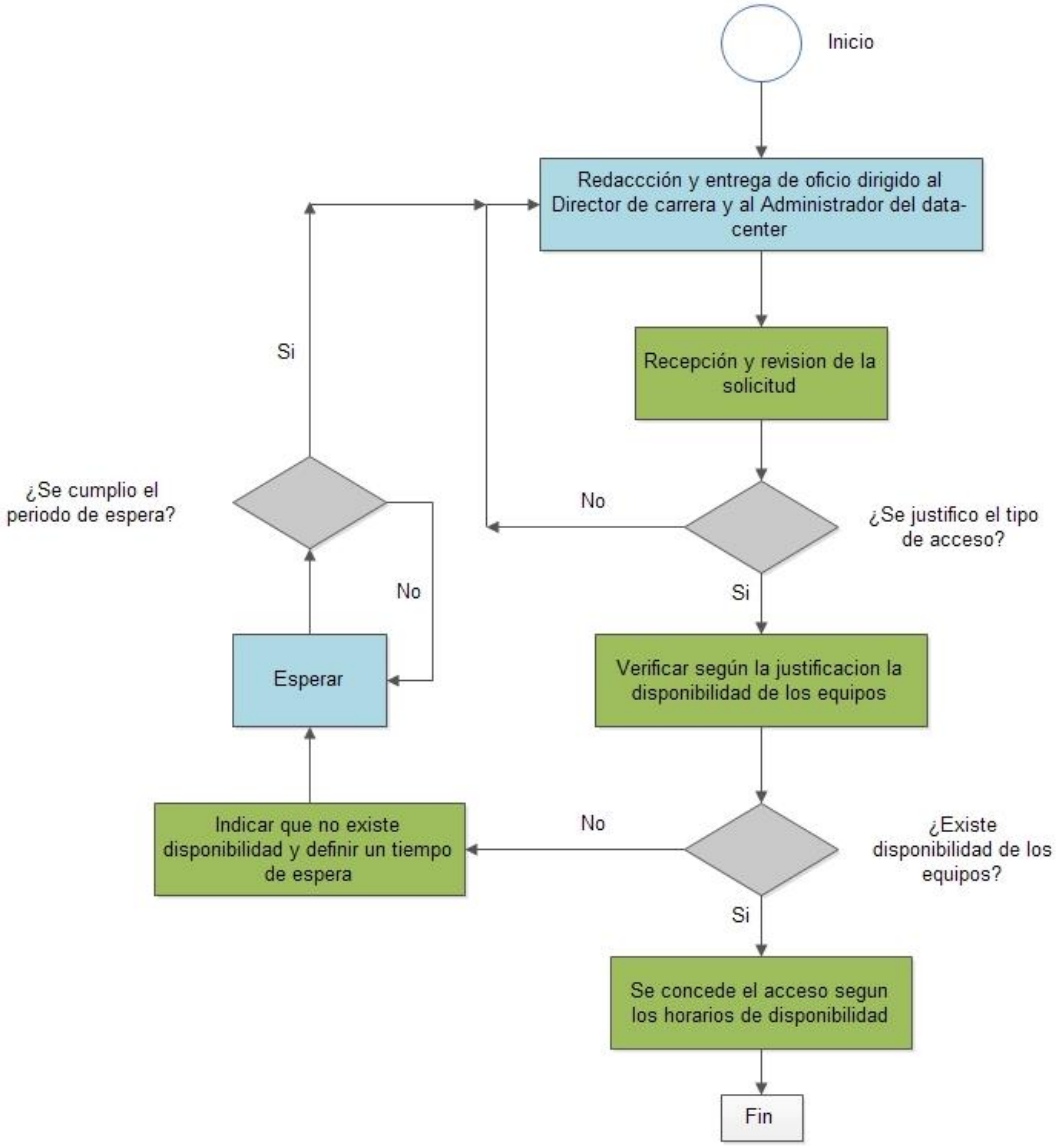


Figura 121. Diagrama de flujo.

Fuente: realizado por el autor

Administrador

Usuario

Desarrollo de Actividades:

N°	Actividad	Descripción	Responsable
1	Usuario redacta la solicitud	El usuario debe delimitar en su oficio dirigido a los administradores de la red y el director de carrera las actividades a realizar dentro del Data-Center, además de los horarios sugeridos para el acceso.	Usuario solicitante
2	Recepción y revisión de la solicitud	Tanto el director de carrera como el administrador del Data-Center reciben la solicitud, revisan si se cumplen los formatos y parámetros	Director de carrera Administrador del Data-Center
3	¿Se justificó el tipo de acceso?	Si la solicitud justifica el acceso se realizara la Actividad 4, caso contrario Actividad 5.	Administrador del Data-Center
4	Verificar según la justificación la disponibilidad de los equipos	Se revisa la justificación escrita por el usuario, la cual debe contener las actividades a realizar y los horarios tentativos. Seguimos a la Actividad 6.	Administrador del Data-Center
5	No se justificó el acceso	Se remite el oficio al usuario solicitando justifique las actividades y horarios tentativos, regresando a la Actividad 1	Administrador del Data-Center Usuario solicitante
6	¿Existe disponibilidad de equipos?	Según la justificación se verifica a que equipos o recursos se solicita acceso según su factibilidad, si existe disponibilidad se realiza la actividad 10, caso contrario la actividad 7.	Administrador del Data-Center
7	Indicar que no existe disponibilidad e indicar un tiempo de espera	Se remite el oficio al usuario solicitante e indica la razón por la cual no se concedió el acceso y se indica el tiempo en que estará disponible el recurso para que se reenvié la solicitud	Administrador del Data-Center
8	Esperar	El usuario espera el tiempo indicado	Usuario solicitante
9	¿Se cumplió el periodo de espera?	En caso de cumplirse se realiza Actividad 1, caso contrarios se desiste o se realiza la Actividad 8	Usuario solicitante

10	Se concede el acceso según los horarios de disponibilidad	Si todos los requisitos se cumplen se asigna los horarios de acceso según la actividad justificada en el oficio	Administrador del Data-Center

Tabla 62. Desarrollo de actividades.
Fuente: realizado por el autor

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Procedimiento:	Mantenimiento y solución de fallos	**Destinatarios:**	Todos los usuarios
	Identificador:	PR-1.0.2	**Fecha de Elaboración:**	

1. Objetivo: Indicar los procesos para la realización de un mantenimiento preventivo y solución de fallos en el Data-Center
2. Alcance: Este procedimiento abarca a los administradores de red del Data-Center que prevean realizar un tipo de mantenimiento o reparación de errores en los equipos.
3. Definiciones:
    - Data-Center: Es el centro de equipos donde se centraliza todos los recursos de la red, servidores, equipos de red, cableado estructurado, racks, sistema de enfriamiento.
    - Administrador de red: Persona encargada del Data-Center, mejor conocido como jefe de TICs.
    - TICs: Tecnologías de información y comunicación.

Diagrama de Flujo:

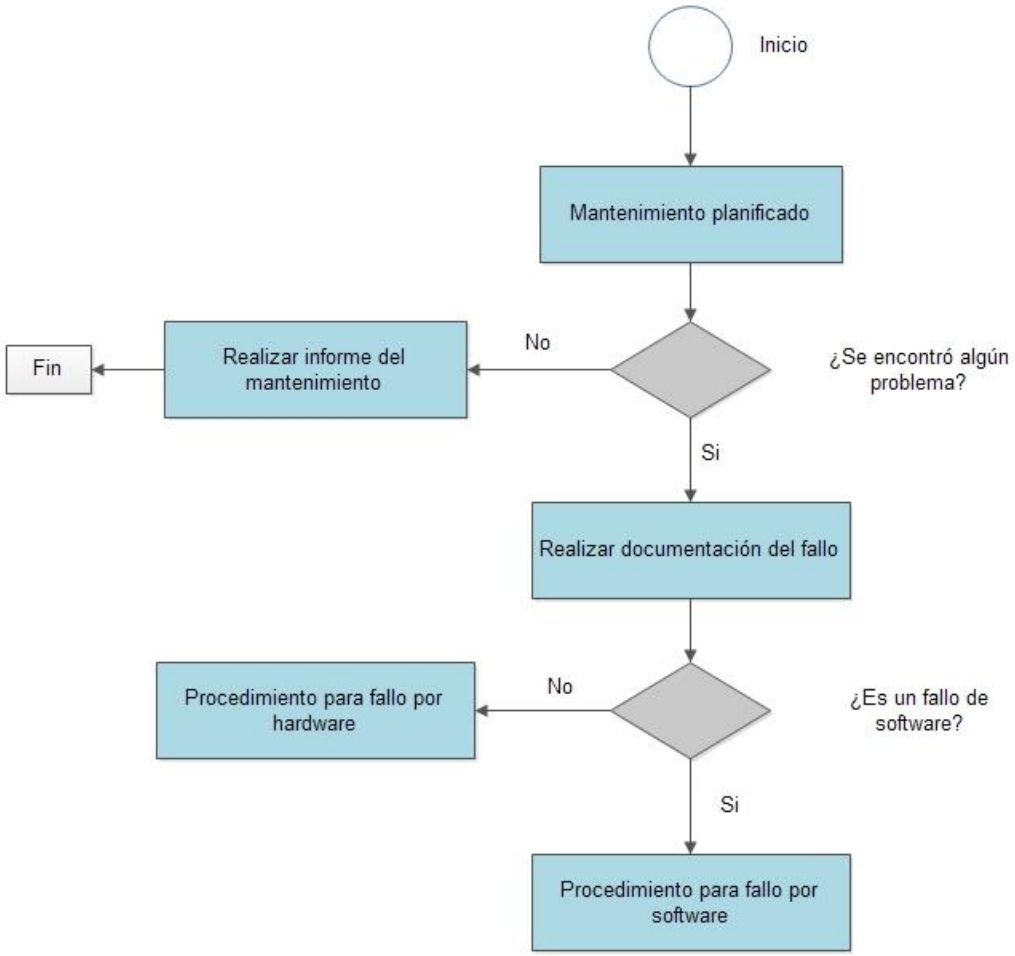


Figura 122. Mantenimiento y solución de fallos.
Fuente: realizado por el autor

Desarrollo de actividades:

N°	Actividad	Descripción	Responsable
1	Mantenimiento planificado	Se realiza la revisión y mantenimiento programado para asegurar el correcto funcionamiento de los equipos	Administrador del Data-Center o técnico encargado
2	¿Se encontró algún problema?	En caso de encontrarlo se procede a la actividad 3, caso contrario A la actividad 7.	Administrador del Data-Center o técnico encargado

3	Realizar documentación del fallo	Se realiza un informe técnico con el fallo encontrado	Administrador del Data-Center o técnico encargado
4	¿Es un fallo de software?	En caso de ser fallo de software se procede a la Actividad 5, caso contrario a la Actividad 6.	Administrador del Data-Center o técnico encargado
5	Procedimiento para fallo por software	Se encamina mediante el procedimiento de fallo por software	Administrador del Data-Center o técnico encargado
6	Procedimiento para fallo por hardware	Se encamina mediante el procedimiento de fallo por hardware	Administrador del Data-Center o técnico encargado
7	Realizar informe del mantenimiento	Se realiza un informe del mantenimiento y se finaliza el proceso	Administrador del Data-Center o técnico encargado

Tabla 63. Mantenimiento y solución de fallos
Fuente: realizado por el autor

PROCEDIMIENTO FALLO POR SOFTWARE

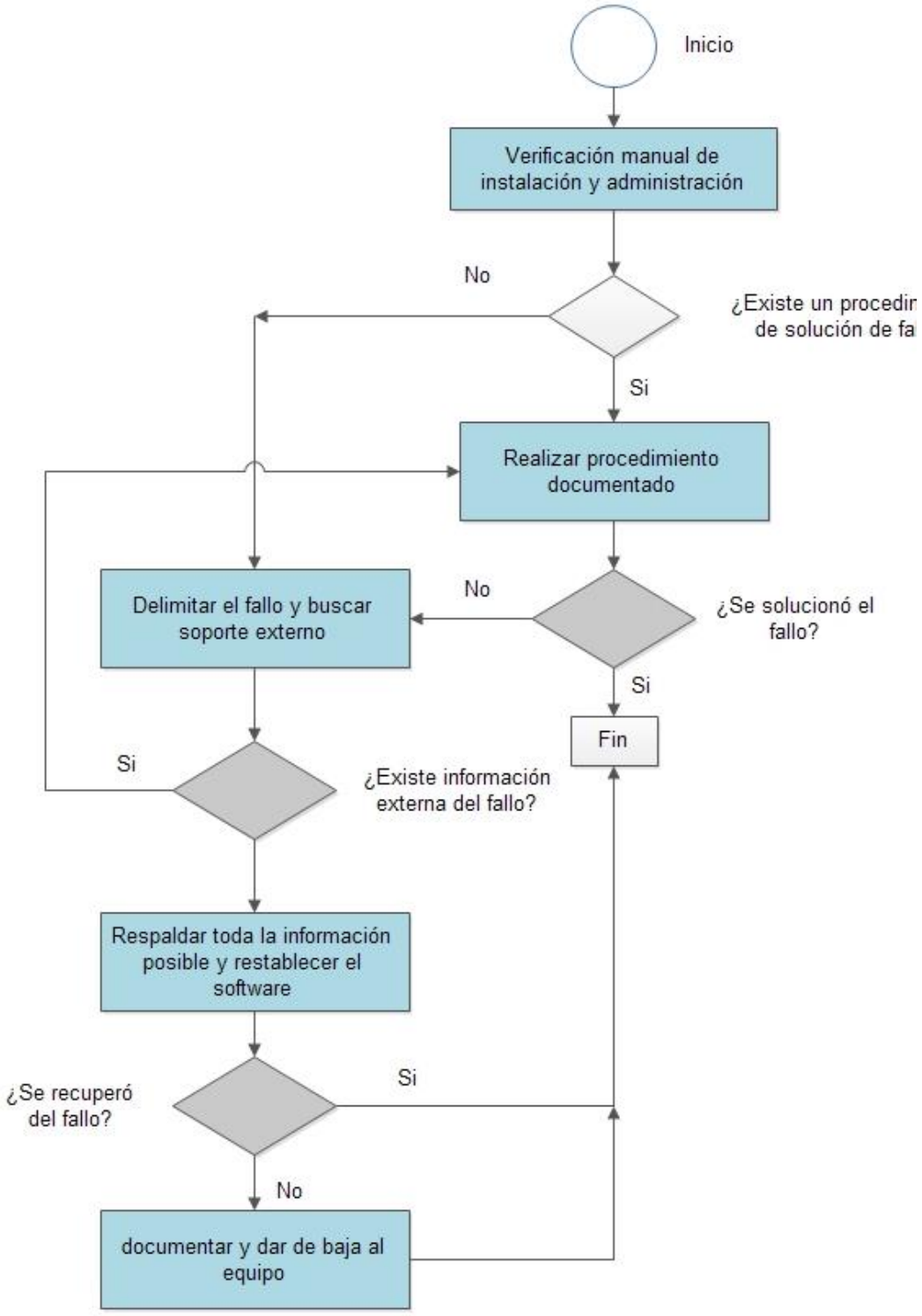
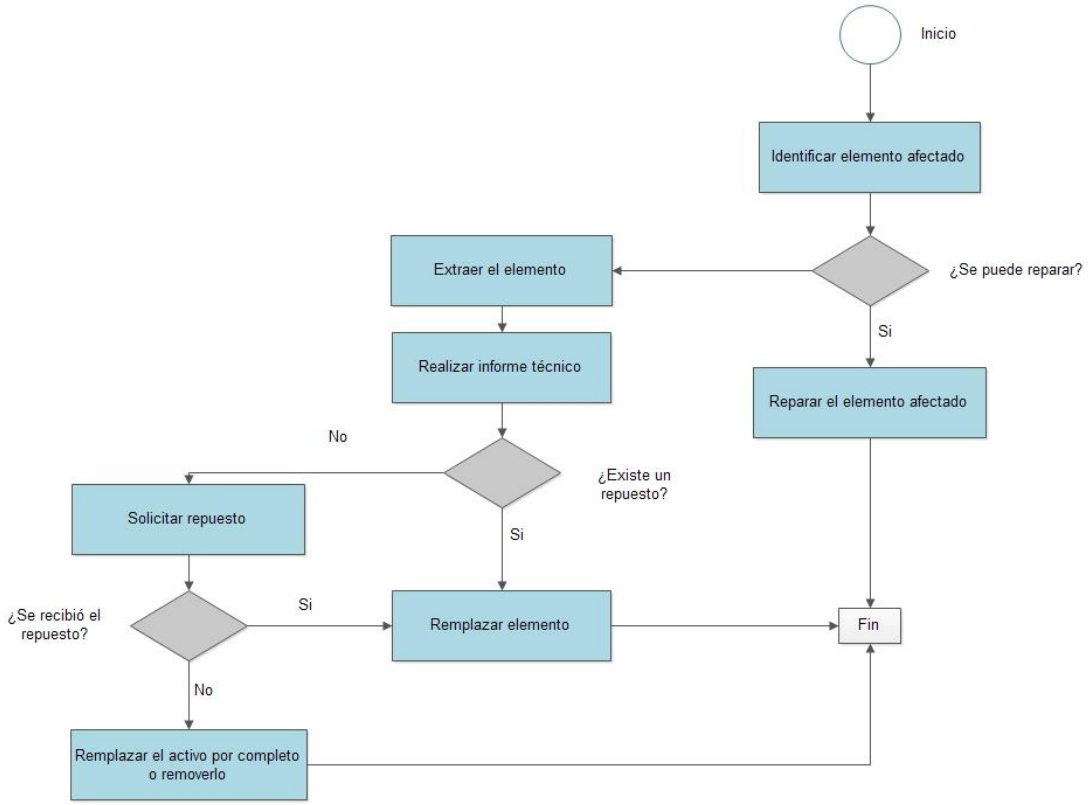


Figura 123. Procedimiento fallo por software
Fuente: realizado por el autor

N°	Actividad	Descripción	Responsable
1	Verificación manual de instalación y administración	Se revisara el manual de isntalacion y adminsitracion del equipo de red o servidor	Usuario solicitante
2	¿Existe un procedimiento de solución de fallo?	En caso de existir un procedimiento se procede a la Actividad 3, caso contrario a la Actividad 5.	Director de carrera Administrador del Data-Center
3	Realizar procedimiento documentado	Se procede a seguir los pasos del manual de administrador o el de instalacion.	Administrador del Data-Center
4	¿Se solucionó el fallo?	En caso que se solucionara el fallo se procede a finalizar el proceso.	Administrador del Data-Center Usuario solicitante
5	Delimitar el fallo y buscar soporte externo	Se delimita el fallo mediante código de error y se procede a buscar informacion externa por medio de la compañía proveedora o bibliotecas digitales	
6	¿Existe información externa del fallo?	En caso de encontrar informacion del fallo procedemos a la Actiidad 3, caso contrario a la Actividad 7.	Administrador del Data-Center
7	Respaldar toda la información posible y restablecer el software	Identificar la informacion importante dentro del activo para proceder a respaldarla para luego restablecer el software afectado.	
8	¿Se recuperó del fallo?	En caso de resultar finaliza el proceso, caso contrario se procede a la Altividad 9.	Administrador del Data-Center
9	Documentar y dar de baja al equipo	Se documenta el proceso realizado en el activo para justificar su eliminación.	

Tabla 64. Procedimiento fallo por software
Fuente: realizado por el autor

PROCEDIMIENTO POR HARDWARE



.

Figura 124. Procedimiento por hardware
Fuente: realizado por el autor

N°	Actividad	Descripción	Responsable
1	Identificar elemento afectado	Se procederá a delimitar el equipo afectado y a su vez el elemento que esta defectuoso	Técnico encargado
2	¿Se puede reparar?	En caso que el elemento se pueda reparar se procede a la Actividad 3, caso contrario a la Actividad 4.	Técnico encargado
3	Reparar el elemento afectado	Se realiza la reparación del elemento de manera cuidadosa, evitando poner en riesgo la integridad del activo	Técnico encargado o administrador del Data-Center
4	Extraer el elemento	Se extrae el elemento afectado sin afectar la integridad del activo	Tecnico encargado

5	Realizar informe técnico	Se realiza un informe técnico del elemento extraído	Técnico encargado o administrador del Data-Center
6	¿Existe un repuesto?	En caso de existir se procede a la Actividad 7, caso contrario se procede a la Actividad 8	Administrador del Data-Center
7	Remplazar el elemento	Se remplazara el activo en caso de tener disponible y se finaliza el proceso.	Técnico encargado
8	Solicitar repuesto	Si no se tiene disponibilidad del repuesto se procede a solicitarlo	Técnico encargado
9	¿Se recibió el repuesto?	En caso de recibirlo procedemos a la Actividad 7, caso contrario se procede a la actividad 10	Administrador del Data-Center
10	Remplazar el activo por completo o removerlo	Se pretende cambiar todo el activo o removerlo del Data-Center junto con todas sus actividades realizando un plan de contingencia	Técnico encargado o administrador del Data-Center

Tabla 65. Procedimiento por hardware
Fuente: realizado por el autor

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Procedimiento:	Remoción de activo	**Destinatarios:**	Todos los usuarios
	Identificador:	PR-1.0.4	**Fecha de Elaboración:**	

1. Objetivo: Definir los procesos para la remoción de un activo dentro del Data-Center
2. Alcance: Este procedimiento será realizado por el técnico encargado mediante la supervisión del administrador del Data-Center para la remoción de equipos obsoletos o defectuosos.
3. Definiciones:

- Data-Center: Es el centro de equipos donde se centraliza todos los recursos de la red, servidores, equipos de red, cableado estructurado, racks, sistema de enfriamiento.
- Administrador de red: Persona encargada del Data-Center, mejor conocido como jefe de TICs.
- TICs: Tecnologías de información y comunicación.

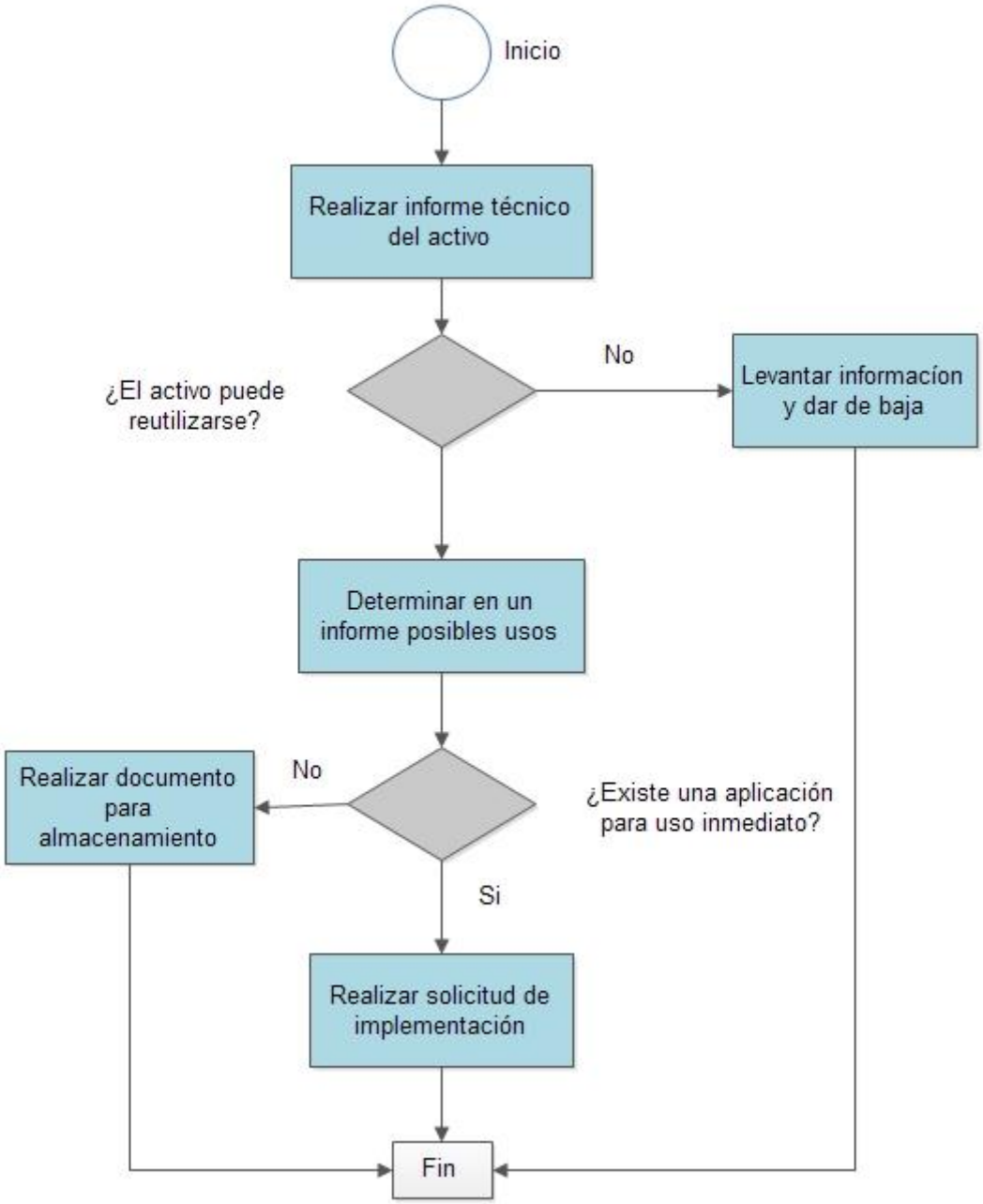


Figura 125.Remoción de activo
Fuente: realizado por el autor

N°	Actividad	Descripción	Responsable
1	Realizar informe técnico del activo	Se procede a realizar un informe que detalle todas las características con las que cuenta el activo.	Administrador del Data-Center
2	¿El activo puede reutilizarse?	En caso de que el activo pueda utilizarse pasamos a la Actividad 4, caso contrario a la Actividad 3.	Administrador del Data-Center

3	Determinar en un informe posibles usos	En base a las características del activo se busca posibles utilidades	Administrador del Data-Center
4	¿Existe una aplicación para uso inmediato?	En caso de existir una aplicación para usar el activo se procede a la Actividad 5, caso contrario Actividad 6.	Administrador del Data-Center
5	Realizar solicitud de implementación	Se realiza una solicitud para utilizar el activo en la implementación inmediata	Técnico encargado
6	Realizar documentos para almacenamiento	Se realiza un documento general de características del activo para almacenarlo en bodega y tener respaldo por si se lo requiere.	Administrador del Data-Center
7	Levantar información y dar de baja	Se realiza un informe técnico que constate que el activo será removido permanentemente y no se puede reutilizar.	Administrador del Data-Center

Tabla 66.Remoción de activo
Fuente: realizado por el autor

	FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS			
	Procedimiento:	Implementación de Activo	**Destinatarios:**	Todos los usuarios
	Identificador:	PR-1.0.3	**Fecha de Elaboración:**	

1. Objetivo: Realizar el procedimiento de implementación de un activo dentro del Data-Center
2. Alcance: Este procedimiento va dirigido para cualquier persona incluida en el grupo estudiantil, docente o administrativo de la facultad de ingeniería y ciencias aplicadas.
3. Definiciones:
    - Data-Center: Es el centro de equipos donde se centraliza todos los recursos de la red, servidores, equipos de red, cableado estructurado, racks, sistema de enfriamiento.

- Administrador de red: Persona encargada del Data-Center, mejor conocido como jefe de TICs.
- TICs: Tecnologías de información y comunicación.

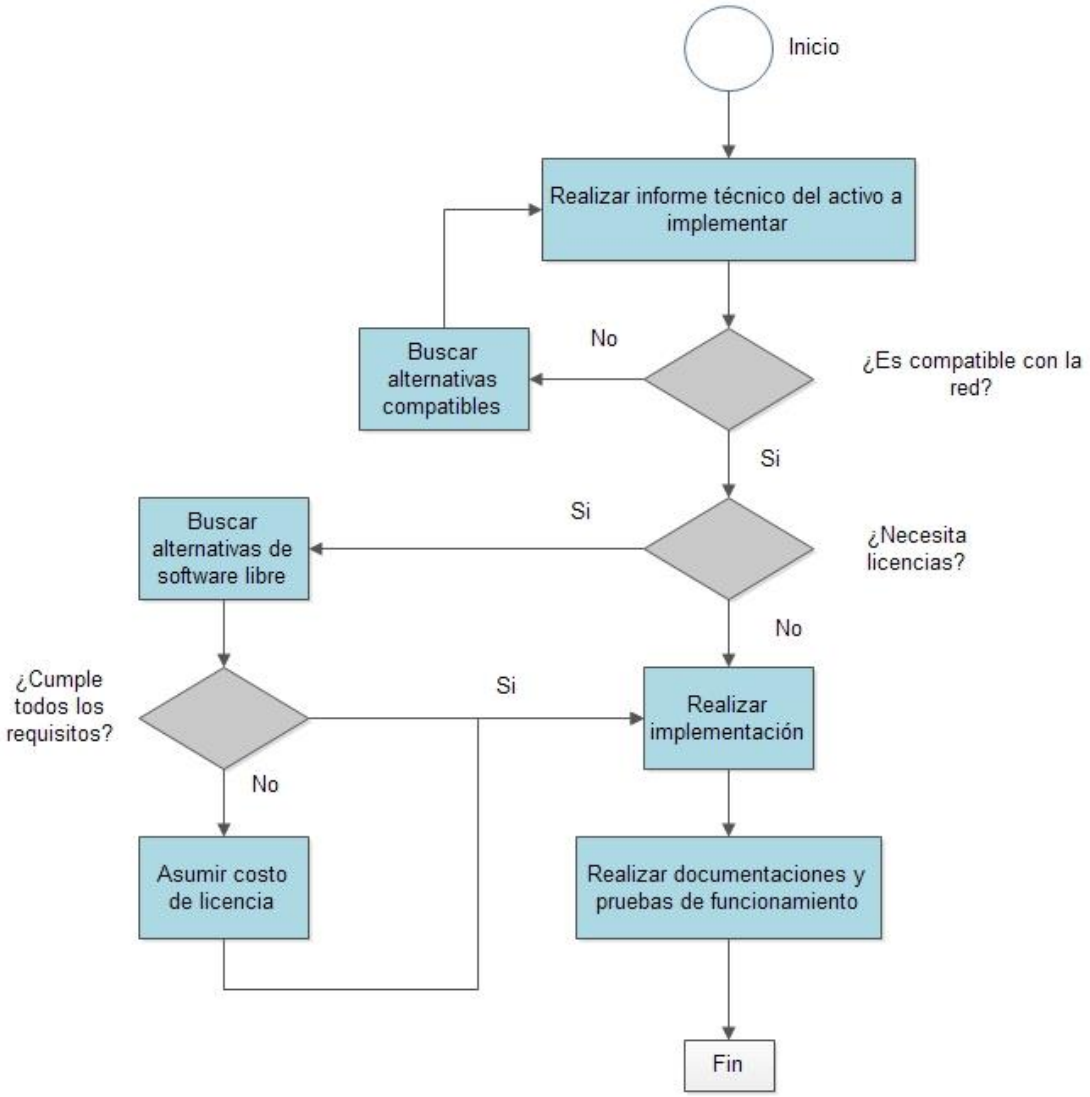


Figura 126. Implementación de activo
Fuente: realizado por el autor

N°	Actividad	Descripción	Responsable
1	Realizar informe técnico del activo	Se realiza el informe técnico del activo que se quiere implementar	Estudiante, docente y administrador del Data-Center
2	¿Es compatible con la red?	En caso de ser compatible se procede a la Actividad 4, caso contrario a la Actividad 3.	Estudiante, docente y administrador del Data-Center
3	Buscar alternativas compatibles	Se buscará una alternativa compatible con los equipos implementados en la red y se procede a la Actividad 1.	Estudiante, docente y administrador del Data-Center
4	¿Necesita licencia?	En caso de contar con licencia pasamos a la Actividad 5, caso contrario a la Actividad 8.	Estudiante, docente y administrador del Data-Center
5	Buscar alternativas de software libre	Si llegara a darse el caso de necesitar licencia se buscará una alternativa en software libre	Estudiante, docente y administrador del Data-Center
6	¿Cumple todos los requisitos?	En caso de hacerlo con software libre se procede a la Actividad 8, caso contrario a la Actividad 7	Estudiante, docente y administrador del Data-Center
7	Asumir costo de licencia	Al descartar alternativas libres en caso de ser necesario se asumirá el costo de licencia	Estudiante, docente y administrador del Data-Center
8	Realizar implementación	Se realiza la implementación del equipo	Estudiante, docente y administrador del Data-Center
9	Realizar documentaciones y pruebas	Una vez implementado se procederá con las pruebas de funcionamiento y su respectivo informe técnico	Estudiante, docente y administrador del Data-Center

Figura 127. Implementación de activo
Fuente: realizado por el autor

Anexo 18: Instalación Endian Firewall

Se realiza la grabación del ISO del software firewall a utilizar en un cd para la instalación del equipo, al momento de iniciar el arranque del equipo se presiona F9 para seleccionar el medio de arranque en este caso el CD.

Paso 1: Al seleccionar el Cd aparecerá la pantalla de la imagen, en donde se selecciona el idioma que utilizaremos en la instalación.

Figura 128. *Selección de Lenguaje Endian*
Fuente: realizado por el autor

Paso 2: en la imagen se puede observar que nos indica la ruta donde se grabara el sistema operativo, además que utilizara todo el disco duro y lo particionara según la configuración requerida.

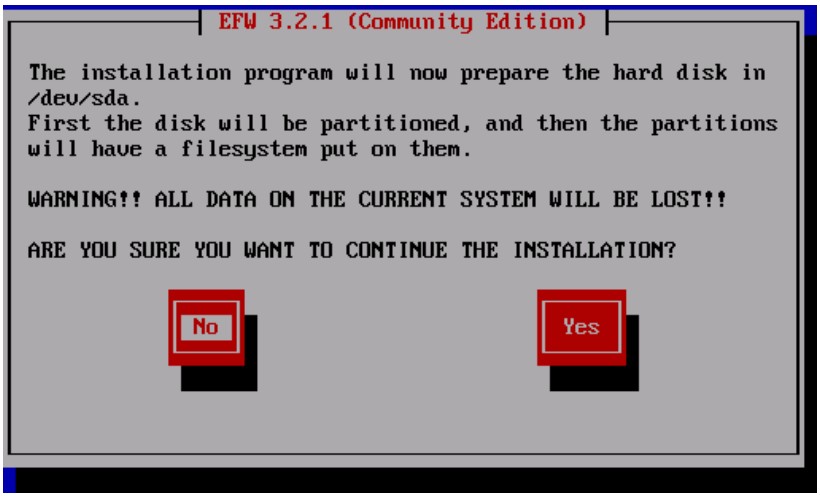


Figura 129.Aceptación de Formateo de Disco Duro Endian
Fuente: realizado por el autor

Paso 3: Se inicia el proceso de configuración asignando los permisos de root

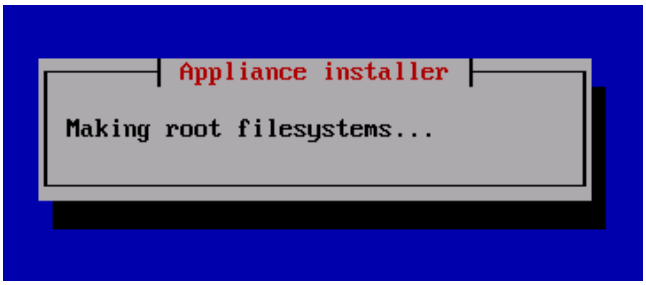


Figura 130. Generación de archivos de sistema Endian
Fuente: realizado por el autor

Paso 4: Se acepta o niega la conexión por puerto serial en caso de no contar con acceso a la tarjeta de red.

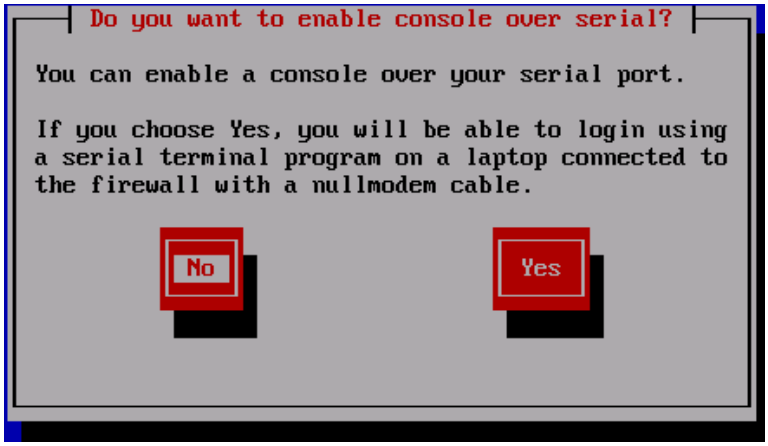


Figura 131. Activación de comunicación por puerto Serial
Fuente: realizado por el autor

Paso 5: Se selecciona el interfaz de red por el cual ingresaremos a configuración web del software.

Figura 132. Selección de ip para acceso a interfaz web y SSH Endian
Fuente: realizado por el autor

Paso 6: Se procede a la instalación con los parámetros básicos configurados

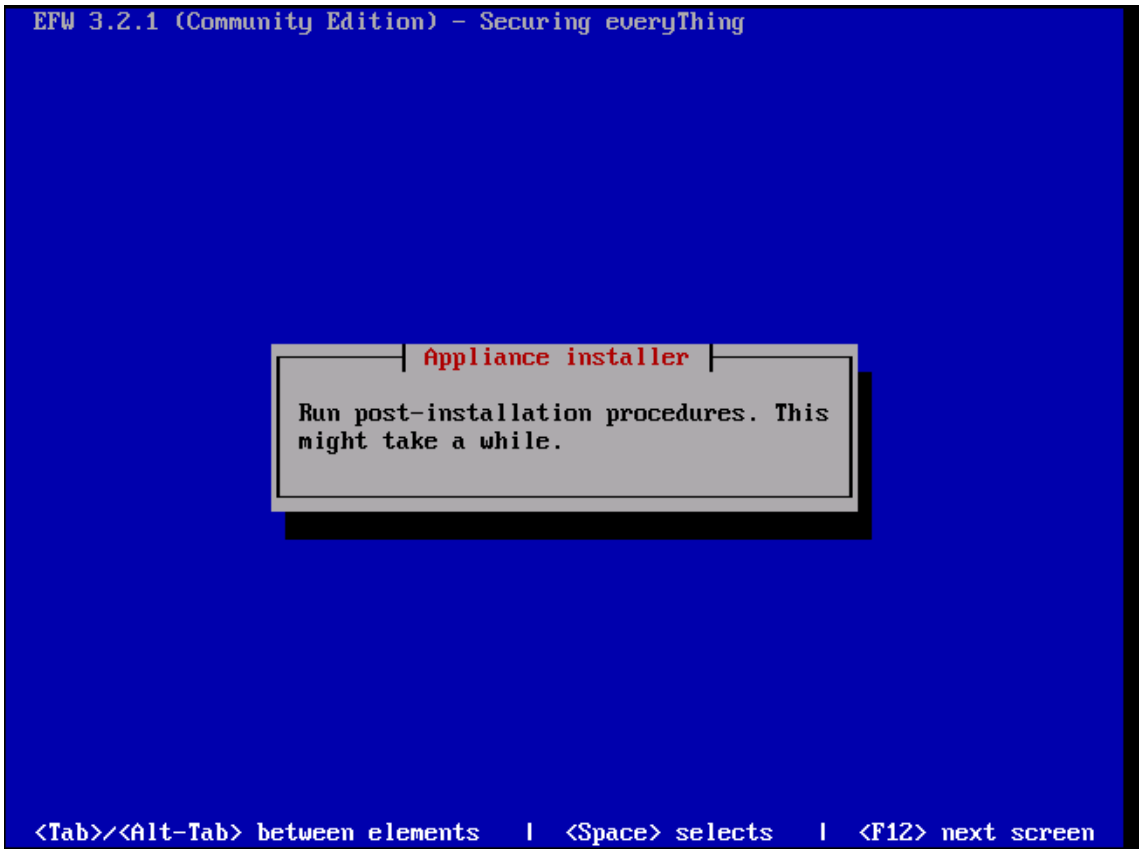


Figura 133. *Aplicando la configuración Endian*
Fuente: realizado por el autor

Paso 7: Al finalizar la instalación se indica la ip por la cual se accederá al interfaz web de endian, se acepta y el sistema se reiniciará.

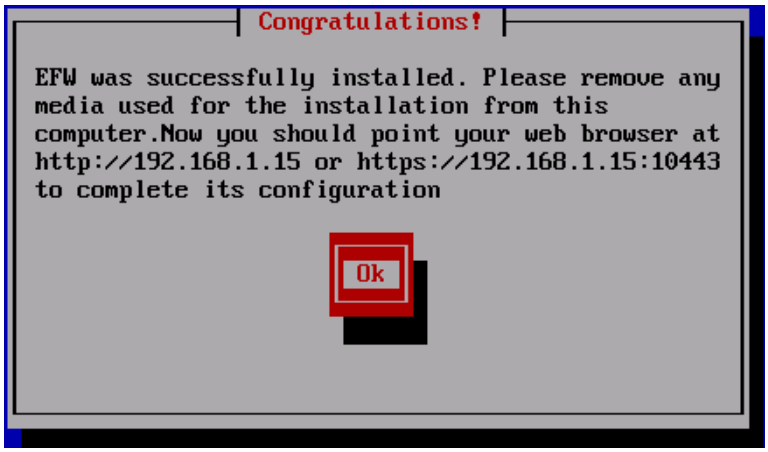


Figura 134. *Mensaje de configuración exitosa Endian*
Fuente: realizado por el autor

Anexo 19: Matriz de Riesgos Situación Final

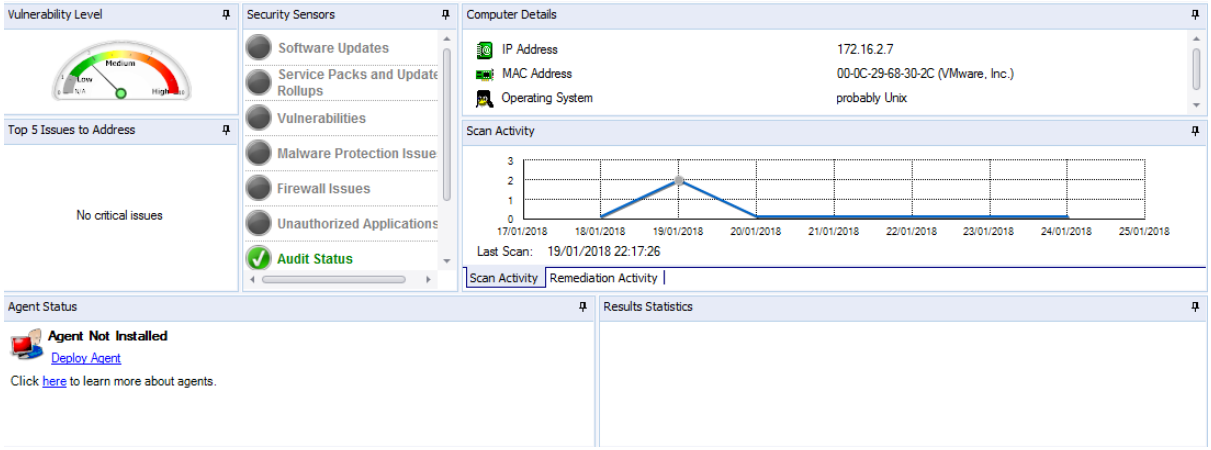
Matriz de Análisis de Riesgo

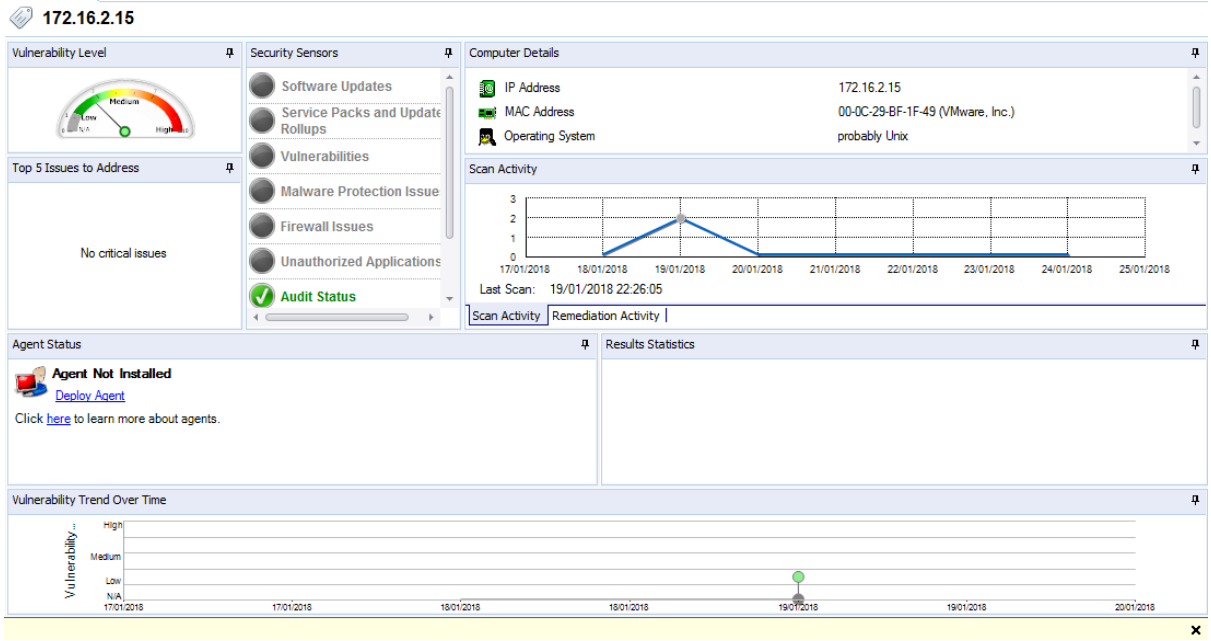
Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

Equipos Data Center	Clasificación: Disponibilidad	Clasificación: Integridad	Clasificación: Confidencialidad	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Origen Humano (Accidental): Errores de los usuarios	Errores del administrador	Errores de monitorización	Errores de configuración	Difusión de software dañino	Errores de encaminamiento	Errores de secuencia	Escapes de información	Alteración accidental de la información	Destrucción de la información	Fugas de información	Vulnerabilidades de los programas	Errores de mantenimiento/actualiza	Errores de mantenimiento/actualiza	Caída del sistema por agotamiento de recursos	Perdida de equipos
					2	2	1	2	1	1	1	2	2	1	1	3	2	2	2	2
IBM Systemx3200 M2 (Radius)	4	3	2	3	6	6	3	6	3	3	3	6	6	3	3	9	6	6	6	6
HP Proliant DL360 G9 (Openstack)	3	4	4	4	8	8	4	8	4	4	4	8	8	4	4	12	8	8	8	8
HP Proliant ML150 G5 (Opina)	4	4	4	4	8	8	4	8	4	4	4	8	8	4	4	12	8	8	8	8
IBM Systemx3500 M4 (Reactivos ó moodle)	4	4	4	4	8	8	4	8	4	4	4	8	8	4	4	12	8	8	8	8
IBM Systemx3500 M4 (DSpace)	3	3	3	3	6	6	3	6	3	3	3	6	6	3	3	9	6	6	6	6
PC tipo Clon H8M-S1 (Biométricos)	4	3	3	3	6	6	3	6	3	3	3	6	6	3	3	9	6	6	6	6
Switch de Core Catalyst 4506-E	4	2	3	3	6	6	3	6	3	3	3	6	6	3	3	9	6	6	6	6
RouterBoard 1100 Mikrotik	4	2	2	3	6	6	3	6	3	3	3	6	6	3	3	9	6	6	6	6
Switch de Distribución 3Com	2	1	1	1	2	2	1	2	1	1	1	2	2	1	1	3	2	2	2	2
Switch de Distribución Linsys	2	1	1	1	2	2	1	2	1	1	1	2	2	1	1	3	2	2	2	2
Switch Distribución inalámbrica QPCOM	3	1	1	2	4	4	2	4	2	2	2	4	4	2	2	6	4	4	4	4

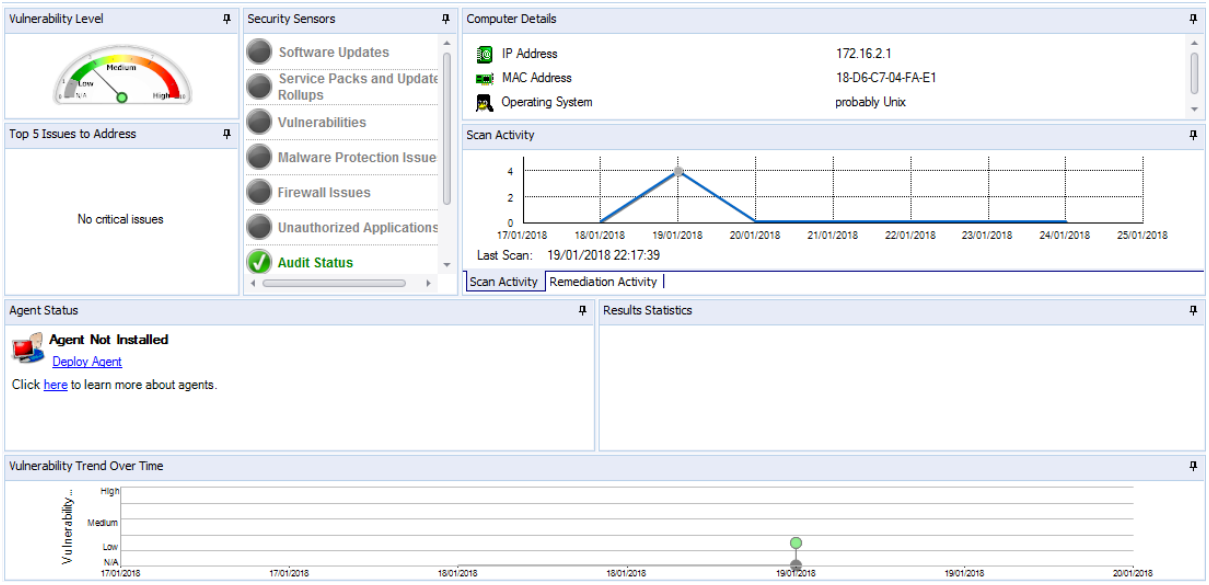
Equipos Data Center	Origen Humano (Deliberado): Manipulación de la configuración	Suplantación de la identidad del usuario	Abuso de privilegios de acceso	Uso no previsto	Difusión de software dañino	Re-encaminamiento de mensajes	Alteración de secuencia	Acceso no autorizado	Repudio	Modificación deliberada de la información	Destrucción de la información	Divulgación de información	Manipulación de programas	Manipulación de los equipos	Denegación de servicio	Robo	Ataque destructivo
	1	1	2	2	1	2	1	1	2	2	1	2	2	1	2	1	1
IBM Systemx3200 M2 (Radius)	3	3	6	6	3	6	3	3	6	6	3	6	6	3	6	3	3
HP Proliant DL360 G9 (Openstack)	4	4	8	8	4	8	4	4	8	8	4	8	8	4	8	4	4
HP Proliant ML150 G5 (Opina)	4	4	8	8	4	8	4	4	8	8	4	8	8	4	8	4	4
IBM Systemx3500 M4 (Reactivos ó moodle)	4	4	8	8	4	8	4	4	8	8	4	8	8	4	8	4	4
IBM Systemx3500 M4 (DSpace)	3	3	6	6	3	6	3	3	6	6	3	6	6	3	6	3	3
PC tipo Clon H8M-S1 (Biométricos)	3	3	6	6	3	6	3	3	6	6	3	6	6	3	6	3	3
Switch de Core Catalyst 4506-E	3	3	6	6	3	6	3	3	6	6	3	6	6	3	6	3	3
RouterBoard 1100 Mikrotik	3	3	6	6	3	6	3	3	6	6	3	6	6	3	6	3	3
Switch de Distribución 3Com	1	1	2	2	1	2	1	1	2	2	1	2	2	1	2	1	1
Switch de Distribución Linsys	1	1	2	2	1	2	1	1	2	2	1	2	2	1	2	1	1
Switch Distribución inalámbrica QPCOM	2	2	4	4	2	4	2	2	4	4	2	4	4	2	4	2	2

Anexo 20: Resultados GFI Languard





172.16.2.1


Vulnerability Level
Medium
Low
N/A
High
Top 5 Issues to Address
No critical issues
Security Sensors
Software Updates
Service Packs and Update Rollups
Vulnerabilities
Malware Protection Issue
Firewall Issues
Unauthorized Applications
Audit Status
Computer Details
IP Address
172.16.2.1
MAC Address
18-D6-C7-04-FA-E1
Operating System
probably Unix
Scan Activity
4
2
0
17/01/2018
18/01/2018
19/01/2018
20/01/2018
21/01/2018
22/01/2018
23/01/2018
24/01/2018
25/01/2018
Last Scan: 19/01/2018 22:17:39
Scan Activity
Remediation Activity
Agent Status
Agent Not Installed
Deploy Agent
Click here to learn more about agents.
Results Statistics
Vulnerability Trend Over Time
Vulnerability
High
Medium
Low
N/A
17/01/2018
17/01/2018
18/01/2018
18/01/2018
19/01/2018
19/01/2018
20/01/2018

Glosario

- **Anti-Debug /tidebugger:** Se trata del conjunto de técnicas que los virus emplean para evitar ser investigados. (KASPERSKY, 2017)
- **Ataque dirigido / Targetted attack:** Son ataques silenciosos e imperceptibles dirigidos específicamente contra una persona. (CERTuy, 2013)
- **Autoencriptación**: Operación mediante la cual un virus codifica (cifra) parte de su contenido, o éste en su totalidad. Esto, en el caso de los virus, dificulta el estudio de su contenido. (KASPERSKY, 2017)
- **Ataque de fuerza bruta / Brute force attack:** Este simple y ya antiguo ataque (aunque se sigue usando) consiste en la utilización de un archivo que contiene todas las combinaciones alfanuméricas y de símbolos posibles para probar el dato a buscar (usuarios, contraseñas, etc.) hasta dar con una coincidencia. (AVAST, 2015)
- **Backdoor / Puerta trasera:** Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario. (AVAST, 2015)
- **Bomba lógica:** Es un programa, en principio de apariencia normal e inofensiva, que puede actuar provocando acciones dañinas, al igual que cualquier otro virus. (Informáticos, 2015)
- **Bot:** Deriva de la palabra 'robot'. Se trata de un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario. (CERTuy, 2013)
- **Bot herder (propietario de bots):** Es la persona o el grupo propietario que controla las redes de bots. También se le llama "bot master" o "zombie master". (CERTuy, 2013)
- **Botnet:** Red o grupo de ordenadores zombies, controlados por el propietario de los bots. El propietario de las redes de bots da instrucciones a los zombies. (AVAST, 2015)

- **Cavity:** Técnica utilizada por algunos virus y gusanos para dificultar su localización. (Informáticos, 2015)
- **Cifrado / Autocrifrado:** Es una técnica utilizada por algunos virus que se codifican a sí mismos (o parte de ellos), para tratar de evitar a los antivirus.
- **Compañía / Virus de compañía / Spawning**: Se trata de un tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos. (Pérez, 2014)
- **Condición de activación (Trigger):** Son las condiciones bajo las cuales un virus se activa o comienza a realizar sus acciones en el ordenador infectado. (Informáticos, 2015)
- **Cracker:** A diferencia del hacker, el cracker quiere romper los sistemas con fines maliciosos, muchas veces económicos, para su propio beneficio personal. (Informáticos, 2015)
- **Crimeware:** Todo aquel programa, mensaje o documento utilizado para obtener beneficios económicos fraudulentamente, perjudicando al usuario afectado o a terceras partes, y de forma directa o indirecta. (Marion AGÉ, 2015)
- **DansGuardian:** Es un software de filtro de contenido, diseñado para controlar el acceso a sitios web. (AVAST, 2015)
- **DMZ:** Una zona desmilitarizada o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. (Marion AGÉ, 2015)
- **DHCP:** Es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes. (Marion AGÉ, 2015)

- **DoS / Denegación de servicios**: Es un ataque, causado en ocasiones por los virus, que evita al usuario la utilización de ciertos servicios (del sistema operativo, de servidores Web, etc). (Marion AGÉ, 2015)
- **DdoS / Denegación de servicios distribuida**: Es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios ordenadores, contra un servidor. (Marion AGÉ, 2015)
- **DNS Poisoning:** Es una situación creada de manera maliciosa o no deseada que provee datos de un servidor de nombres de dominio (DNS) que no se origina de fuentes autoritativas DNS. (AVAST, 2015)
- **Derechos de propiedad intelectual (DPI):** Son derechos legales que protegen las creaciones y/o invenciones, resultantes de la actividad intelectual en el campo industrial, científico, literario o artístico. (KASPERSKY, 2017)
- **Dropper:** Es un fichero ejecutable que contiene varios tipos de virus en su interior.
- **DSpace:** Es un software de código abierto que provee herramientas para la administración de colecciones digitales, y comúnmente es usada como solución de repositorio bibliográfico institucional. (IBM, 2017)
- **EPO (Entry Point Obscuring):** Técnica para infectar programas mediante la cual un virus intenta ocultar su punto de entrada para evitar ser detectado. (Informáticos, 2015)
- **Exploit:** Es una técnica o un programa que aprovecha un fallo o hueco de seguridad, una vulnerabilidad existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática. (Informáticos, 2015)
- **Firewalls:** Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas del mismo. (KASPERSKY, 2017)

- **Fingerprinting:** Es el proceso de recopilación de información que permite identificar el sistema operativo en el ordenador que se tiene por objetivo. (Tori, 2008)
- **Flooder:** Programa que envía el mismo mensaje o texto de manera reiterada y masiva, pretendiendo así producir un efecto de saturación, colapso o inundación en sistemas de correo como MSN Messenger. (Pérez, 2014)
- **Footprinnting:** Es el primer paso y el paso más importante que toman los Hacker para obtener toda la información que necesitan antes de lanzar un ataque
- **Google Hacking**: Es una técnica en informática que utiliza operadores para filtrar información en el buscador de Google. (CERTuy, 2013)
- **Gusano (Worm:**Este tipo de malware usa los recursos de red para distribuirse. Su nombre implica que pueden penetrar de un equipo a otro como un gusano. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta. (Tori, 2008)
- **Hacker:** Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras o a un experto en cualquier otro campo, aunque no esté relacionado con la informática. (Informáticos, 2015)
- **Hardering:** Hardening o bastionado, en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. (AVAST, 2015)
- **Hijacker:** Se encargan de "secuestrar" las funciones de nuestro sistema cambiando la página de inicio y búsqueda y/o otros ajustes del navegador. Estos pueden ser instalados en el sistema sin nuestro consentimiento al visitar ciertos sitios web mediante controles ActiveX o bien ser incluidos por un troyano. (AVAST, 2015)

- **Honeypot:** Un honeypot, o sistema trampa o señuelo, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante. (Pérez, 2014)
- **IDS:** Un sistema de detección de intrusiones (o IDS de sus siglas en inglés Intrusion Detection System) es un programa de detección de accesos no autorizados a un computador o a una red. (Pérez, 2014)
- **IMAP:** El protocolo de acceso a mensajes de Internet, es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. (IBM, 2017)
- **Ingeniería social:** Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. (KASPERSKY, 2017)
- **IPS:** Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. (Marion AGÉ, 2015)
- **Keylogger (Capturador de teclado):** Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan los datos que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etc.). (KASPERSKY, 2017)
- **Kolab:** es una suite de herramientas colaborativas basadas en Software Libre con capacidades para las funciones de correo electrónico, calendario, notas y tareas compartidas. (AVAST, 2015)
- **Malware:** El malware (del inglés “malicious software”), es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. (Marion AGÉ, 2015)

- **Man-in-the-middle(MITM):** Se trata de un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
- **MRTG:** es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red.
- **Nat:** es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. (Pérez, 2014)
- **Nuke (ataque):** Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado. (Tori, 2008)
- **OSINT (Open Source Intelligence):** es la disciplina encargada de la adquisición, tratamiento y posterior transformación en inteligencia de la información conseguida a partir de fuentes de carácter público como prensa, radio, televisión, internet, informes de diferentes sectores y en general. (IBM, 2017)
- **Payload:** es el conjunto de datos transmitidos que es en realidad el mensaje enviado. (Pérez, 2014)
- **Phising:** Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. (Tori, 2008)
- **Pentesting:** Una prueba/test de penetración o pentesting es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. (Pablo González, 2015)
- **Postfix:** es un servidor de correo de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención

de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail. (IBM, 2017)

- **Rootkits**: es un programa diseñado para proporcionar a los hackers acceso administrativo a un equipo sin su conocimiento. (KASPERSKY, 2017)
- **Ransomware:** Es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. (KASPERSKY, 2017)
- **Riskware:** Muestran publicidad al usuario. La mayoría de programas adware son instalados a software distribuido gratis. La publicidad aparece en la interfaz. A veces pueden colectar y enviar los datos personales del usuario. (KASPERSKY, 2017)
- **SMTP:** El Simple Mail Transfer Protocol o "protocolo para transferencia simple de correo", es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. (IBM, 2017)
- **Spear phishing:** Utiliza las técnicas del phishing pero se trata de un ataque dirigido lanzado contra un objetivo concreto. El autor que origina este tipo de ataque, nunca recurrirá al spam para conseguir una avalancha masiva de datos personales de los usuarios. (Pérez, 2014)
- **Spyware:** El spyware o programa espía es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. (KASPERSKY, 2017)
- **Squid:** es un servidor proxy para web con caché. Es una de las aplicaciones más populares y de referencia para esta función, software libre publicado bajo licencia GPL.

- **Ssh:** Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera. (Marion AGÉ, 2015)

- **TIC:** Tecnologías de Información y Comunicación a menudo, se usa el término para referirse a cualquier forma de hacer cómputo.
- **Troyano:** En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado. (Informáticos, 2015)
- **Virus de boot.-** Es un virus que afecta al sector de arranque de los discos de almacenamiento. (Informáticos, 2015)
- **Vpn:** Virtual Private Network es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. (Tori, 2008)
- **Zero-day attack(0-day attack).-** Ataque con el propósito de ejecutar código malicioso contra un zero-day.Un ataque de este tipo se considera una de las herramientas más peligrosas del mundo en una guerra informática. (Marion AGÉ, 2015).

BIBLIOGRAFÍA

- Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing For IT Security Teams.* Chichester: WILEY.
- Amutio Gomez, M. A. (2012). MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. En M. A. Amutio Gomez, *MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo* (pág. 175). Madrid: Ministerio de Hacienda y Administraciones Públicas.
- AVAST. (2015). *avast.com*. Obtenido de https://www.avast.com/es-es/c-spyware
- CERTuy. (23 de Abril de 2013). *cert.uy*. Obtenido de https://www.cert.uy/inicio/sobre_seguridad/glosario/
- Escudero, J. (10 de 12 de 2017). *Emprendedores*. Obtenido de Emprendedores: http://www.emprendedores.es/gestion/como-calcular-tu-precio-hora
- IBM. (2017). *bm.com*. Obtenido de https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzair/rzairemcommnd.htm
- Informáticos, D. (2015). *delitosinformaticos.info*. Obtenido de http://www.delitosinformaticos.info/delitos_informaticos/glosario.html
- KASPERSKY. (2017). *kaspersky*. Obtenido de https://support.kaspersky.com/sp/viruses/general/614
- Marion AGÉ, F. E. (2015). *Seguridad Informatica: Ethical Hacking.* Barcelona: Ediciones ENI.

- OVH. (24 de 10 de 2017). *OVH Innovation is Freedom*. Obtenido de OVH Innovation is Freedom: https://www.ovh.com
- Pablo González, G. S. (2015). *Pentesting con Kali 2.0.* Madrid: 0XWORD.
- Pérez, P. G. (2014). *Ethical Hacking.* Madrid: 0xWORD.
- Tori, C. (2008). *Hacking Ético.* Buenos Aires: Maestroianni.
- UNE 71504:2008. (2008). *Metodología de análisis y gestión de riesgos para los sistemas de información.*
- Uygur, S. U. (2014). *Penetration testing with BackBox.* Birmingham: Packt Publishig.