UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

INFORME DE TRABAJO PROFESIONAL

DISEÑO E IMPLEMENTACIÓN DE LA ESTRUCTURA BASE DEL SOPORTE TÉCNICO Y SEGURIDAD INFORMÁTICA, PROYECTO DE TRABAJO.

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

PRESENTA:

RENE ALEJANDRO GUEVARA CANALES

AVAL:

ING. HESAÚL SÁNCHEZ RAYA

ASESOR:

ING. CRUZ SERGIO AGUILAR DÍAZ

CIUDAD UNIVERSITARIA 19/Septiembre/2014

Contenido

Índice de Figuras

Índice de Tablas

CAPÍTULO 1:

Introducción

Antes de comenzar el desarrollo de este proyecto describiré algunas de las actividades realizadas en trabajos anteriores y que me han permitido tener una idea de manera general de lo que es el ámbito laboral y lo importante que es la relación entre personas laboralmente hablando para cumplir las tareas que se realizan en una empresa u organización.

Experiencia profesional

Encuestador telefónico

La función desempeñada durante el periodo que laboré como encuestador telefónico pude apreciar de manera funcional las características de un sistema informático encargado de llamadas controladas por computadora.

El trato con personas era algo cotidiano, los problemas y las negativas lo eran también, con lo que pude aprender algunas técnicas para lograr entablar un diálogo y lograr respuestas positivas por parte de las personas que se entrevistaban. En el tipo de trabajo actual es muy útil ese tipo de experiencia ya que se trata con clientes y el trato debe de ser cordial y amable.

Becario en la Unidad de Servicios de Cómputo Académico (UNICA)

Durante mi paso en la Facultad de Ingeniería realicé mi servicio social en una de las salas de cómputo de ésta, perteneciente a la Unidad de Servicios de Cómputo Académico (UNICA).

Actividades:

- Instalación de sistemas operativos
- Instalación de programas diversos para el uso del alumnado de la Facultad.
- Clonación de sistemas completos de computadoras.
- Administración de cuentas de usuarios.
- Administración y mantenimiento de las computadoras.

A continuación se describirá el reporte laboral para la titulación por trabajo profesional.

El informe que se presenta a continuación tiene como objetivo explicar y describir las actividades y programas que me permitieron el diseño y la implementación de los procesos, herramientas y pasos a seguir para desarrollar las bases del soporte y la seguridad de la información, perteneciente al área de **Redes y Seguridad**, lugar donde me desenvuelvo en el ámbito profesional.

El interés de diseñar la estructura para proporcionar el servicio de soporte técnico a los diferentes equipos con los que se trabaja es la base para la seguridad de la información. Surge de las necesidades que se requieren para realizar con mayor eficiencia las tareas programadas, así como también de esta manera generar un aporte en beneficio de la empresa.

Comenzaré por hacer mención de los antecedentes del proyecto, en donde se describe la forma en cómo se desarrollaba el proceso y la problemática que generaba para las diferentes áreas que conforman la estructura de trabajo.

CAPÍTULO 2:

Descripción de proyectos realizados

Ambiente virtual para servidores

Objetivo. Implementar un ambiente para establecer los servicios internos y realizar pruebas para nuevos servicios que se desarrollan día con día.

Debido a la necesidad de establecer diferentes servicios se optó por instalar un software de virtualización de cómputo, el cual facilita el manejo de máquinas virtuales y adicionalmete permite la libertad de añadir y remover dichas máquinas. Las limitaciones de los servidores que pueden crearse dependen del hardware del equipo en el que se instaló y de la versión del programa de virtualización.

Este programa cuenta con diferentes aplicaciones para la gestión de ambientes virtuales, la aplicación Vcenter permite la gestión de diferentes host de ESXi y de las máquinas virtuales que estos contengan en una sola interfaz gráfica.

La instalación se realiza de forma similar a la de un sistema operativo, la administración de la herramienta se hace desde la consola del servidor en donde se puede realizar todos los ajustes del modo en que se otorga el servicio, para poder obtener el servicio se debe hacer desde el cliente instalando el software que proporciona la interfaz web del propio servidor por medio de su dirección IP, es así que toda gestión de las máquinas virtuales se realiza desde el cliente mediante una interfaz gráfica.

Dentro de las versiones de los virtualizadores se cuenta con una capaz de administrar a las demás, con una interfaz similar a las versiones comúnes, esta versión cuenta con la diferencia de tratarse de un servicio y no comportarse como sistema operativo, permite la migración de maquinas virtuales entre servidores “arrastrando y soltando”, básicamente cuenta con las mismas funciones de un servidor común con la capacidad de ordenar a los demás.

Monitoreo de red

Objetivo. Tener el conocimiento constante del estado del servicio de la red interna así como de los servicios que se proporcionan, con la finalidad de detectar actividad inusual o sospechosa de los equipos de la empresa.

Las aplicaciones y servicios en la red se han incrementado con el paso del tiempo, por lo cual el monitoreo de redes se ha convertido en una actividad cada vez más importante y cotidiana para prevenir, detectar y/o evitar problemas.

Se instlaron algunos IDS (Sistemas de Detección de Intrusos, por sus siglas en inglés), con la finalidad de tener un mayor conocimiento de lo que ocurre en la red de la empresa en términos de seguridad, se cuenta también con un sistema de monitorización que vigila los servidores y los servicios que estos proveen.

El monitoreo por medio de los IDS se lleva a cabo mediante la configuración de un puerto en los switches, habilitando un puerto en modo espejo el cual es utilizado para enviar copias de los paquetes de red, con lo que el sistema de detección puede examinar el tráfico de la red sin representar un puno de quiebre en la infraestructura de la red local.

La supervisión de los servidores y de sus servicios de realiza con una arquitectura cliente-servidor, el servidor principal es el que se encarga de recibir las peticiones de los distintos clientes los cuales requieren de una configuración con los elementos suficientes para poder establecer la comunicación y por ende su monitoreo.

Las consideraciones para el uso de este tipo de herramientas consiste en el cuidado de amenazas que provienen del exterior, es decir desde internet, pero también se considera que se debe vigilar el comportamiento que se tiene desde el interior de la red local hacia el exterior, por lo que la configuración que se realiza en los dispositivos de monitoreo es con ambos puntos de vista.

Servicios internos

Objetivo. Proporcionar servicios que mejoren, agilicen y ayuden en los procesos y actividades del personal que labora en la empresa.

Dentro de las diferentes actividades que se realizan dentro de la empresa existen ciertos servicios que ayudan a agilizar los procesos y tareas que tiene que realizar el personal de los diferentes departamentos.

Un servidor se dedica a la gestión de documentos, permite el control de comentarios, conversaciones, versiones, edición, etc.. Esto permite la implementación de un repositorio de información que conecte a las personas y la información, gestionar la inteligencia colectiva que aportan los diferente elementos humanos de la compañia.

Este servicio ofrece un interfaz web que permite una interacción más sencilla entre el usuario y el servicio. En la configuración de los diferentes epacios dentro del repositorio se especifica que solo personal autorizado puede accesar a información específica, cada departamento de la empresa tiene sus espacios de trabajo bien definidos y los permisos de cada usuario basados en el puesto que tiene en la empresa.

Otro servicio consta de un gestor de tareas a realizar, incluye un sistema de seguimiento de incidentes, calendario de actividades, un glosario, etc.. Este servicio tiene como objetivo tener un control sobre las labores de los elementos que integran cada departamento de la compañia, propocionar un tiempo límite para realizar los deberes, hacer cometarios sobre el desarrollo de la actividad y determinar el avance de los proyectos.

Para realizar una configuración o cambio importante, en cualquiera de los servicios internos, que requiera de la intervención de los administradores se debe elaborar una petición por escrito con las especificaciones de lo que se pretende obtener, esta petición es evaluada y por el encargado del departamento de sistemas y el encargado del SOC (Security Operation Center, para más información consultar el Anexo 1).

CAPÍTULO 3:

Diseño e implementación de la estructura base del soporte técnico y seguridad informática

3.1 Organigrama

Dentro de la compañia se tiene una estructura definida sobre los diferentes departamentos que la conforman, la Figura 1.1 muestra el organigrama representando gráficamente las relaciones jerárquicas entre los diferentes puestos existentes.

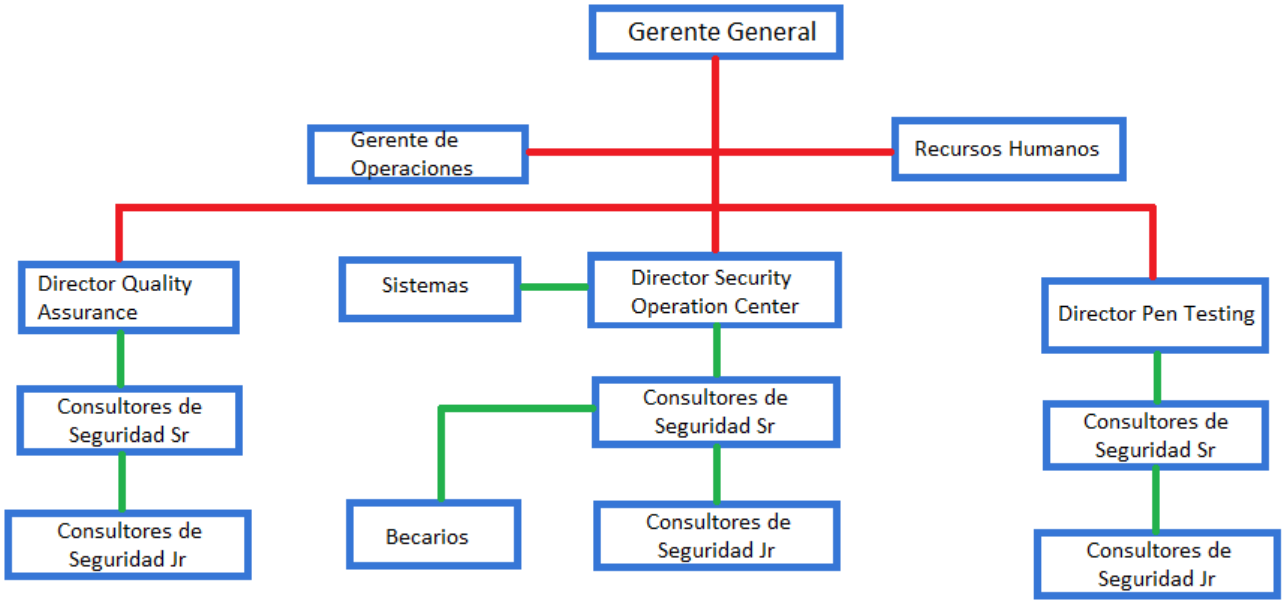


Figura 1. Organigrama.

a) **Gerente General**.- se encarga de la administración de la empresa, es responsable de todos los aspectos del funcionamiento adecuado de los procesos dentro de la empresa, organiza y efectúa la implementación de políticas generales
b) **Gerente de Operaciones**.- maneja las operaciones diarias de la empresa, es responsable de proporcionar asistencia técnica y operativa orientada a la ejecución adecuada de las funciones de las distintas áreas dentro de la

empresa, coordina la ejecución de proyectos y vigila el cumplimiento de las metas de los programas.

c) **Recursos Humanos**.- maneja la parte de los contratos, artículos de oficina, control de asistencia. Elabora y comunica informes periódicos referentes al cumplimiento de metas, cumplimiento de la normativa legal laboral y realizar actividades de seguimiento para el control y aplicación de las mismas.

d) **Director Quality Assurance**.- dirige y administra el área de QA, se encarga de planificar y proponer aplicadas en un sistema de calidad para que los requisitos de calidad de un proyecto o producto sean evaluados.

e) **Director Security Operation Center**.- dirige y administra el área del SOC, se encarga de coordinar a los consultores de seguridad seniors en los distintos proyectos de la empresa, planifica las actividades de los integrantes del área.

f) **Director Pen Testing**.- dirige y administra el área de PT, planifica las actividades de las auditorias de pruebas de penetración, propone recomendaciones para la mejora de los sistemas, coordina a los consultores de seguridad senior del área.

g) **Sistemas**.- planea, organiza, establece y mantiene en operación los sistemas de la empresa en general, administra la configuración y seguridad de la red local, asegura la conectividad entre los servicios y estaciones de trabajo de la empresa y supervisa el mantenimiento preventivo y correctivo de los equipos informáticos.

h) **Consultores de Seguridad Senior**.- maneja los proyectos del área correspondiente proporciona asistencia técnica en las áreas de diseño de sistemas de información, programación y desarrollo de software, estrategias de negocio de la información y el análisis de sistemas.

i) **Consultores de Seguridad Junior**.- realiza diferentes actividades dependiendo el área de trabajo, dirigido por el consultor sr o el director de área.

j) **Becarios**.- mismo perfil del consultor junior.

3.2 Descripción de proyecto

En la Figura 2 se muestra el esquema básico de las etapas que conforman el proyecto, el inicio, el final y un ciclo en el cual se hace una regresión para verificar el funcionamiento.

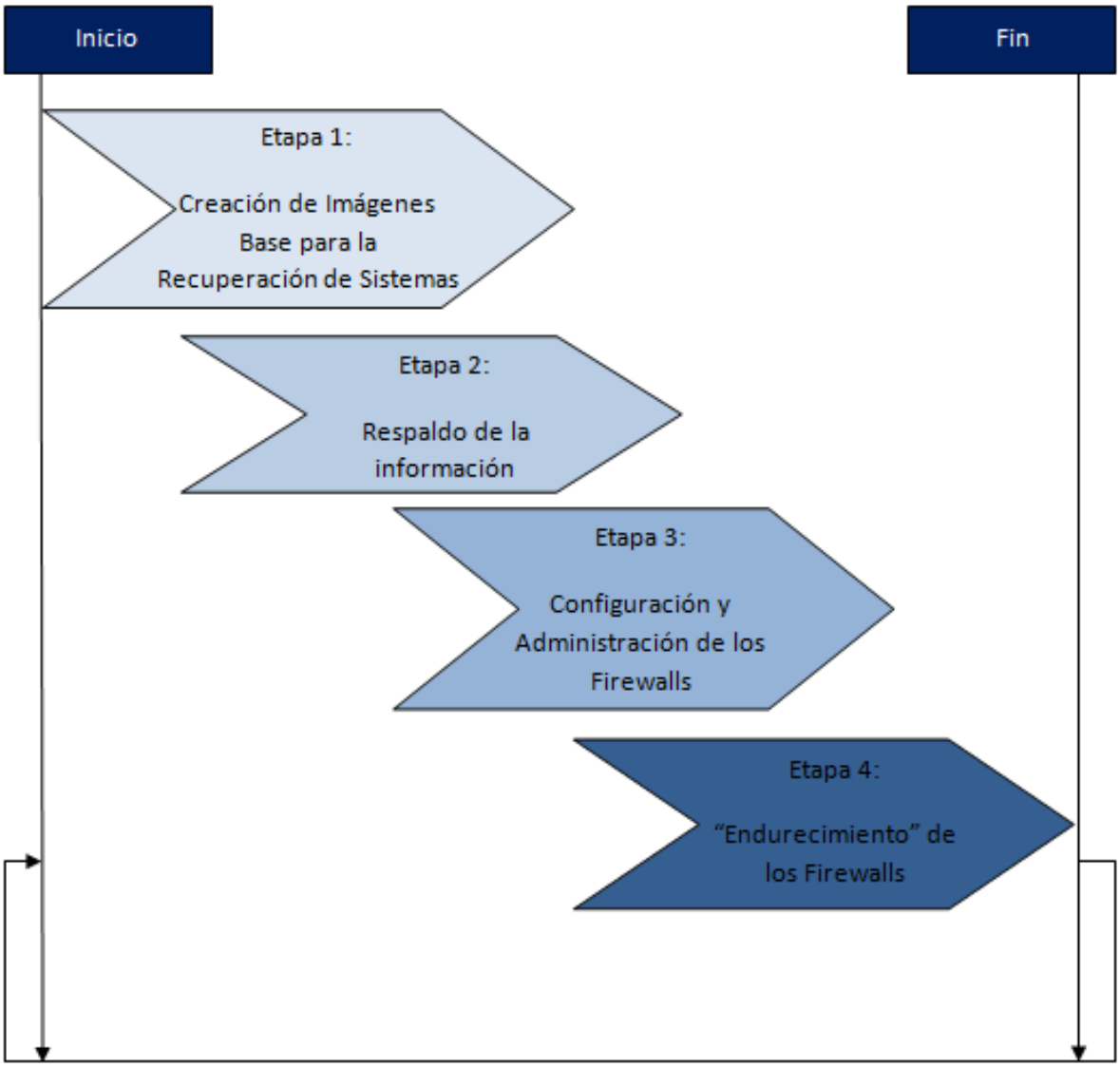


Figura 2. Esquema de las etapas del proyecto.

- **Etapa 1.** Creación de Imágenes Base para la Recuperación de Sistemas

  En esta parte se establece el procedimiento a seguir cuando se quiere crear una imagen del sistema de una computadora, mostrando las diferentes actualizaciones necesarias de los programas en el equipo, utilizando el software “Clonezilla”, así como los pasos a seguir cuando se quiere restaurar una imagen de un sistema previamente hecho con la misma herramienta.

- **Etapa 2.** Respaldo de la información

  En esta parte se establece el procedimiento para el uso de la herramienta “Cobian Backup”, la instalación y la configuración de las diferentes características para definir las tareas que tienen la función de realizar el respaldo requerido de las carpetas y subcarpetas como parte de las políticas de seguridad de la empresa.

- **Etapa 3.** Configuración y Administración de los Firewalls

  En esta parte se muestran las características y las configuraciones realizadas como base de la estructura de seguridad dentro de la empresa, utilizando firewalls de la marca Fortinet.

  La gestión y el manejo que se tiene para aprovechar los diferentes elementos que conforman el sistema dentro de los firewalls, y mantener en óptimas condiciones el funcionamiento y actividades programadas para los firewalls.

- **Etapa 4.** “Endurecimiento” de los Firewalls

  En esta parte se muestra el resultado de la auditoría interna hecha a los firewalls y las conclusiones sobre lo que se debe mejorar y la situación actual del sistema.

3.3 Objetivos del proyecto

El presente informe tiene como propósito demostrar mediante un ejemplo real, el desempeño de las habilidades adquiridas durante el estudio de la carrera de Ingeniería en Computación, además de tomar la esencia de la definición de un ingeniero. Al demostrar las técnicas y habilidades adquiridas durante el tiempo de ejercicio de la profesión dentro del área de mi especialización que es **Redes y Seguridad**, teniendo un desarrollo profesional pleno, en donde el aprendizaje se da diariamente enriqueciendo y fortaleciendo mi formación profesional.

También se describen los procesos de desarrollo realizados en cada etapa del proyecto, explicando de manera detallada y sencilla las actividades y decisiones tomadas con respecto a las diferentes situaciones, buscando siempre las soluciones más eficientes y concretas posibles, dentro de los alcances que tenía cada etapa.

Por cuestiones de políticas de seguridad, protección de datos y confidencialidad de la empresa, sólo se proveerán en este trabajo algunas partes del diseño y del desarrollo del proyecto, **la información o datos aquí utilizados se han cambiado o censurando por protección de la empresa ya que se consideró de carácter sensible y/o confidencial**, y además se refleja un pequeño prototipo de las funcionalidades que tiene un proceso crítico y complejo.

Diseñar la base del soporte técnico brindado dentro de la empresa, a los diferentes sistemas informáticos, principalmente de los equipos de cómputo en las áreas de trabajo, estableciendo una serie de imágenes para la recuperación de los sistemas de cómputo en caso de fallo, y el respaldo de la información generada por parte de los integrantes del SOC (Security Operation Center) por medio de herramientas y procesos diseñados para esta función en particular.

Implementar el debido proceso con el cual se establecen los pasos a seguir para la creación y restauración de la imagen base para la recuperación del equipo afectado, así como el propio proceso a seguir para la elaboración de los respaldos de información.

Configurar las diversas características de los firewalls, mediante al análisis de las necesidades del trabajo a desarrollar por parte de la empresa y la correcta implementación de las funciones requeridas para las actividades realizadas día a día, para establecer la base de la seguridad en la empresa y su trabajo en internet.

Objetivos específicos

- Establecer una de serie de imágenes de respaldo de las computadoras con que realiza su trabajo el personal de la empresa.
- Optimizar el proceso, el tiempo y la eficiencia de la elaboración de los respaldos de la información.
- Implementar un manual de procedimientos en la realización de las imágenes base para la recuperación de sistemas.
- Implementar un manual de procedimientos de actualización de los sistemas.
- Implementar un manual de procedimientos en la realización del respaldo de la información.
- Tener los elementos necesarios para responder eficientemente en caso de algún incidente con equipos dentro de la empresa.
- Establecer algunos controles de seguridad para las actividades cotidianas dentro del SOC.

Antecedentes del proyecto

El presente informe describe el proyecto y las actividades realizadas para el diseño y la implementación de soluciones de las diferentes necesidades de una empresa, llevando a cabo diferentes fases para cada solución realizando una serie de documentaciones en las que se establece el procedimiento a seguido, y el que se debe seguir en caso de que otros miembros del personal requieran emplear las soluciones.

Problemática

Hasta el momento no había alguna forma establecida por parte de la empresa en México, de proporcionar el servicio de soporte técnico, no existía un diagrama de red, no se había establecido un método formal para el respaldo de la información y no se contaba con los firewalls ni mucho menos con una documentación de cómo gestionar ni realizar estas actividades.

Análisis y propuesta de la solución

De acuerdo con las funciones que realizan las diferentes áreas que conforman la empresa, es muy importante el funcionamiento constante de los equipos en las estaciones de trabajo.

La mayoría de la información que se obtiene, crea y maneja es de carácter crítico y su importancia es vital para el accionar de los negocios en la empresa.

La seguridad de la infraestructura de la red es importante en la mayoría de las empresas, por lo que se debe tener una base sólida y confiable para tomarla como punto de partida y poder implementar los servicios necesarios para un óptimo desempeño en el presente y futuro cercano.

Una de las principales preocupaciones en la implementación de la solución es el costo del software y hardware que se podrían llegar a necesitar. Se optó por el uso de software libre en el caso de la creación de las imágenes para la recuperación de los equipos de cómputo y el respaldo de la información.

En la elección del hardware de los firewall se confió en las personas con mayor conocimiento y experiencia en el medio de este tipo de dispositivos, marcas y diferentes modelos.

3.4 Implementación del proyecto

En el proyecto que se presenta a continuación se explica el diseño y la implementación de los procesos, herramientas y pasos a seguir para construir las bases del soporte y la seguridad de la información dentro de la infraestructura de una empresa.

El diseño de una estructura para el servicio de soporte es una función de toda empresa en la cual sus actividades se realizan en sistemas computacionales, la información que se maneja puede o no ser crítica, pero sí tiene una importancia en los procesos de las entidades que las manejan, por lo que es de vital importancia tener un proceso y esquema para la recuperación de los sistemas en caso de fallas o en su defecto el respaldo de la información en caso de no poder recuperarse el contenido de dichos sistemas.

La seguridad de la información es una necesidad que toda empresa tiene estos días, tiene como finalidad la protección de la información y de los sistemas que la contienen, por lo que tener un diseño de sus bases es fundamental, de ahí se desprende el resto de las técnicas y herramientas que se usan para asegurar de la mejor manera la confiabilidad de los procesos y la documentación de las empresas.

En la fase de diseño se siguieron diferentes esquemas previamente establecidos, basados en experiencias anteriores por parte de las personas quienes supervisaron el desarrollo del proyecto, y en las necesidades presentes y algunas consideradas a futuro, con cierta libertad de decidir y proponer ideas propias durante el desarrollo del proyecto.

La implementación de cada una de las etapas del proyecto se probó previamente hasta que el resultado fuera el esperado, con la finalidad de que al momento de ponerlo en producción no hubiera problemas o conflictos con respecto al hardware y al software.

La auditoría interna hecha al sistema de firewall permite obtener una perspectiva de la situación actual del manejo que se tiene sobre los firewalls, de ahí se parte para mejorar en los aspectos más significativos como el acceso por medio de la red interna, los protocolos que utiliza para su administración, los respaldos de configuración, etc., y así reducir el riesgo y las vulnerabilidades del sistema. La auditoría se realizó en base al documento “Auditing fortigate firewall appliance” el cual fue facilitado por el Director de Quality Assurance.

Cada parte del proyecto ha sido probada, ya sea con la intención de probarlas intencionalmente o con situaciones inesperadas en un entorno de pruebas. Los resultados finales han sido satisfactorios.

3.4.1 Alcances

El proyecto cumple con las bases necesarias que se requieren para las actividades dentro del SOC.

El diseño de los diferentes procesos descritos en este proyecto, son únicamente la base y el punto de partida de las actividades concernientes a las diferentes áreas en las que se puedan incluir estas actividades de soporte y respaldo.

El soporte técnico proporcionado se limita a la base de los sistemas y el software que lo acompaña, sin tener responsabilidad en aspectos específicos de las diferentes áreas de desarrollo.

Los métodos implementados para la seguridad de la información se establecieron de acuerdo con procesos previamente establecidos en la empresa y las necesidades consideradas, las actividades o incidentes que se encuentren fuera del esquema, son responsabilidad de la persona que involucrada.

Las diferentes configuraciones de los firewalls se relacionan a las actividades realizadas por los integrantes del SOC, sólo actividades justificadas tienen la prioridad necesaria para efectuar cambios en las reglas.

El endurecimiento de los firewalls se realizó con respecto a las vulnerabilidades mostradas después de una auditoría interna, y sólo en los aspectos que corresponden a las características del modelo de firewall.

3.4.2 Creación de imágenes base para la recuperación de sistemas

Antes de la creación de las imágenes, se debe actualizar todo el software del sistema de uno de los equipos de cómputo para que sea tomado como el punto de partida en la recuperación de los sistemas.

3.4.2.1 Actualización de software

Las actualizaciones no solo corrigen errores de programación, si no también dan soporte a nuevas tecnologías, evitan vulnerabilidades de seguridad, en ocasiones corrigen problemas con las memorias, pero una de sus funciones más importantes es mantener la estabilidad de nuestros sistemas operativos.

Se inició por la actualización del antivirus, tanto el motor y su base de datos como a la última versión disponible.

Las actualizaciones siguientes en realizarse fueron las que el sistema solicitaba, como “java”, “Adobe” y las de Sistema Operativo.

El antivirus “avast!”, tiene una función de actualización de software (software updater), dando click en el botón “analizar”, se muestran los programas que requieren una actualización así como el estado del software en general, dentro de la barra de cada programa se encuentra un botón de “Actualizar”, con el que busca automáticamente las actualizaciones necesarias y las ejecuta.

Una vez que se ha actualizado el software con avast, podemos dar click en el botón “Volver a analizar”, para asegurase de que las actualizaciones han sido exitosas y que no hay alguna otra actualización necesaria.

En la Figura 3 se muestra la interfaz de avast en la que se aprecia el estado de las actualizaciones disponibles.

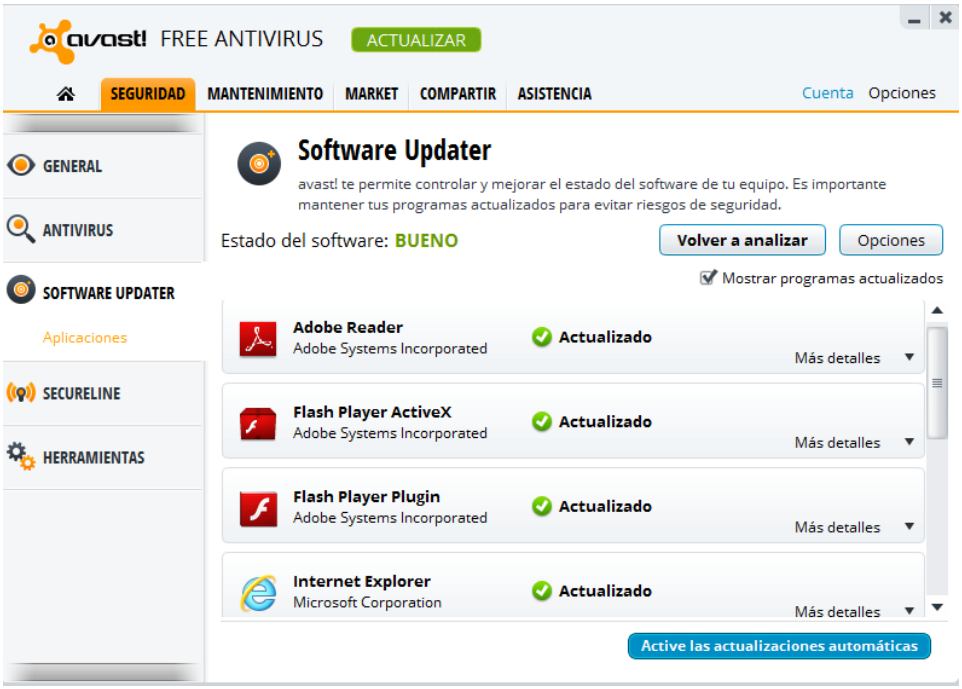


Figura 3. Interfaz de Avast de actualizaciones de software.

En el caso del programa “Mozilla Thunderbird”, no es posible la actualización vía los mensajes de Windows ni con los de avast. Para actualizar este programa se hace desde el menú de aplicaciones de thunderbird, en la figura 4 se muestra la ubicación de dicho menú:

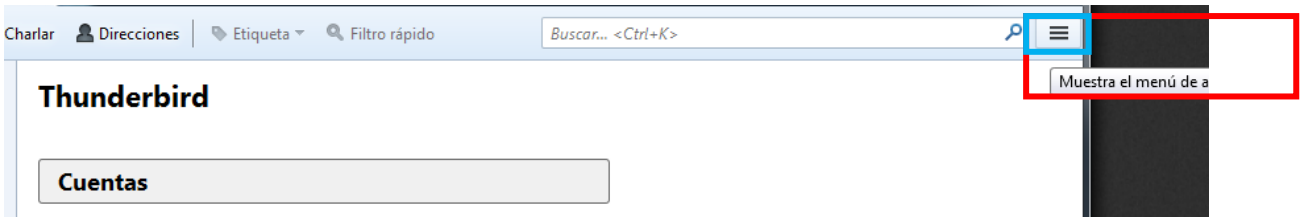


Figura 4. Actualización de Mozilla Thunderbird, menú de aplicaciones.

- En “ayuda”
  - Acerca de Thunderbird
    - Se despliegan las actualizaciones disponibles.

En la Figura 5 se muestra la ventana de “Acerca de Mozilla Thunderbird”, en donde indica el estado de posibles atualizaciones.

Figura 5. Ventana de actualización de Mozilla Thunderbird.

3.4.2.2 Herramientas

Para crear las imágenes de respaldo de las computadoras dentro del SOC (Security Operation Center), se utilizó el programa “Clonezilla”, es un software libre de recuperación ante desastres, sirve para la clonación de discos y particiones. Clonezilla está diseñado por Steven Shaiu y desarrollado por el NCHC Labs en Taiwán. Clonezilla ofrece soporte multicast similares a Norton Ghost Corporate Edition. En la Figura 6 se muestra el logotipo del programa.

Figura 6. Logotipo de Clonezilla.

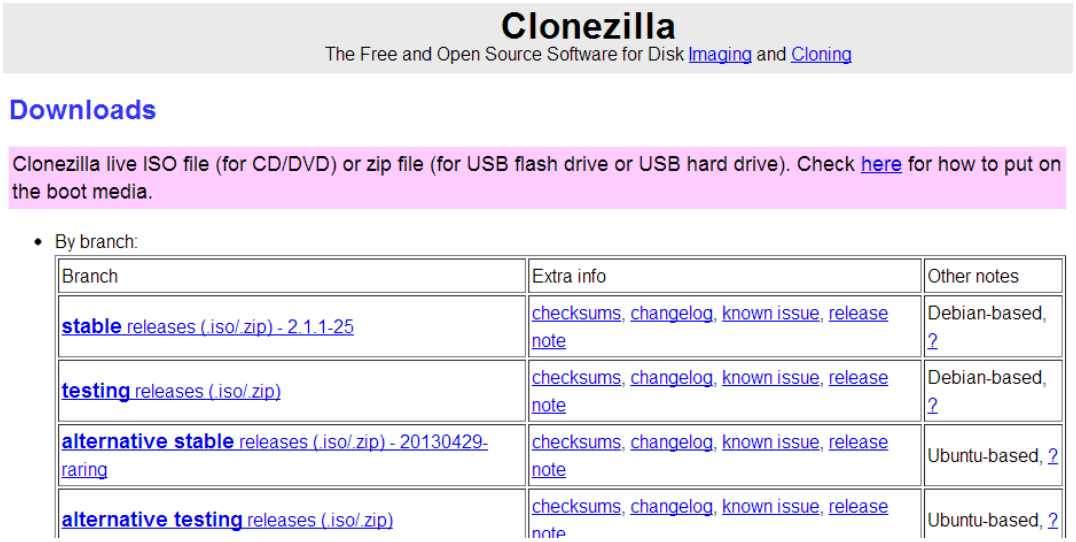
3.4.2.2.1 Elaboración de imágenes base paso a paso

Clonezilla es un software que debe iniciarse desde un live cd o una memoria USB, en éste caso se creó un disco con la imagen .ISO de Clonezilla.

3.4.2.2.1.1. Descarga y creación del live cd para uso de Clonezilla

En un navegador de internet buscar en dónde poder descargar el archivo .ISO de Clonezilla, para este proyecto se descargó de la dirección: http://clonezilla.org/downloads.php

En la Figura 7 se muestra la apariencia de la página oficial de descarga de Clonezilla.



Clonezilla

The Free and Open Source Software for Disk Imaging and Cloning

Downloads

Clonezilla live ISO file (for CD/DVD) or zip file (for USB flash drive or USB hard drive). Check here for how to put on the boot media.

- By branch:

Branch	Extra info	Other notes
stable releases (.iso/.zip) - 2.1.1-25	checksums, changelog, known issue, release note	Debian-based, ?
testing releases (.iso/.zip)	checksums, changelog, known issue, release note	Debian-based, ?
alternative stable releases (.iso/.zip) - 20130429-raring	checksums, changelog, known issue, release note	Ubuntu-based, ?
alternative testing releases (.iso/.zip)	checksums, changelog, known issue, release note	Ubuntu-based, ?

Figura 7. Página oficial de descarga de Clonezilla.

Una vez descargado el software, se debe ubicar el archivo en la carpeta que contenga las descargas, se da click secundario sobre él y presionar en “Grabar imagen en disco” como se muestra en la Figura 8.

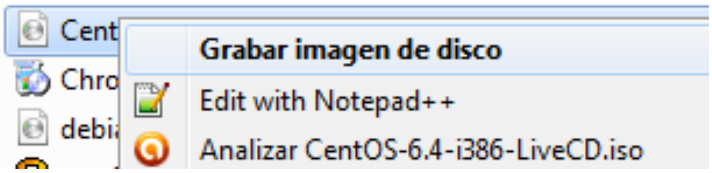


Figura 8. Crear el live cd.

3.4.2.2.1.2. Crear imagen paso a paso

Insertar el live cd que contiene el software de Clonezilla, reiniciar la computadora y arrancar el sistema desde el disco. En la Figura 9 se muestra la pantalla de inicio al arrancar el sistema con Clonezilla.

Figura 9. Pantalla de inicio de Clonezilla.

3.4.2.2.1.2.1 Selección de versión de Clonezilla

Los creación de la imagen del sistema de una computadora se lleva a cabo con una serie de sencillos pasos, Clonezilla presenta un sistema de elección de opciones para configurar la tarea que se desea efectuar, los pasos mas sencillos son los siuientes:

- Seleccionar “Clonezilla live (Default settings, VGA 800x600)”
- Elegir mapa de teclado según arquitectura
- Distribución física del teclado: Latin American
- Iniciar Clonezilla: Start_Clonezilla Iniciar Clonezilla
- Escoger modo: Disco a/desde imagen
- Indicar origen: Usar dispositivo local
- Conectar dispositivo externo (si aún no se ha conectado)
- Montar dispositivo repositorio de imagen: <Elegir dispositivo externo>
- Directorio para la imagen de Clonezilla: /Directorio_Superior_en_el_Dispositivo_local
- Seleccionar modo de ejecución para el asistente: Beginner Modo Principiante
- Elegir modo: Save disk

- Nombre de imagen: Elegir el nombre de la imagen que se creará del disco o partición
- Seleccionar disco: Seleccionar el disco (o partición) de la que se quiere crear la imagen de respaldo
- Comprobar sistema: Elegir si se quiere comprobar y reparar el sistema
- Comprobar imagen: Después de que se grabe la imagen, elegir si se quiere comprobar si la imagen se puede restaurar.
- Grabar disco

En la Figura 10 se muestra como se despliega el progreso de la creación de una imagen.

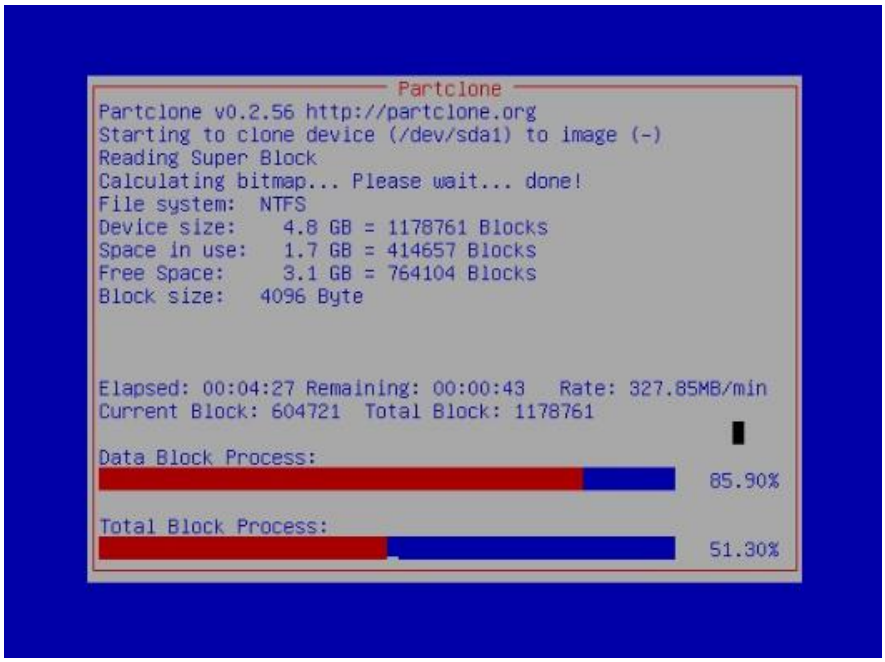


Figura 10. Pantalla de progreso de la creación de la imagen del sistema.

Si en ninguno de los pasos anteriores se mostró algún error, la imagen ha sido creada exitosamente. Para comprobar que no hay errores, se puede restaurar la imagen en alguna computadora y verificar que el sistema no tenga fallas.

3.4.2.2.2 Restaurar imagen paso a paso

Insertar el disco con la imagen de Clonezilla, reiniciar la computadora y arrancar desde el disco.

3.4.2.2.2.1 Selección de versión de Clonezilla

Los creación de la imagen del sistema de una computadora se lleva a cabo con una serie de sencillos pasos, Clonezilla presenta un sistema de elección de opciones para configurar la tarea que se desea efectuar, los pasos mas sencillos son los siuientes:

- Seleccionar “Clonezilla live (Default settings, VGA 800x600)”
- Elegir mapa de teclado según arquitectura
- Distribución física del teclado: Latin American
- Iniciar Clonezilla: Start_Clonezilla Iniciar Clonezilla
- Escoger modo: Disco a/desde imagen
- Indicar origen: Usar dispositivo local
- Conectar dispositivo externo (si aún no se ha conectado)
- Montar dispositivo repositorio de imagen: <Elegir dispositivo externo>
- Directorio para la imagen de Clonezilla: /Directorio_Superior_en_el_Dispositivo_local
- Seleccionar modo de ejecución para el asistente: Beginner Modo Principiante
- Elegir modo: Restoredisk

En la Figura 10 se muestra la opción a elegir al momento de querer restaurar un sistema con una imagen creada.

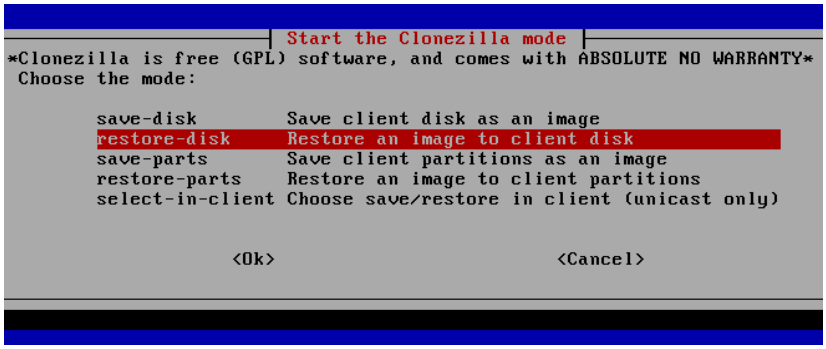


Figura 11. Restoredisk.

- Archivo de imagen: Elegir el archivo de la imagen a restaurar
- Seleccionar disco: Seleccionar el disco (o partición) en donde se quiere restaurar el sistema con la imagen de respaldo que se tiene creada.

Si en ninguno de los pasos anteriores se mostró algún error, la imagen ha sido creada exitosamente. Para comprobar que no hay errores, se puede restaurar la imagen en alguna computadora y verificar que el sistema no tenga fallas.

3.4.3 Respaldo de la información

3.4.3.1 Herramienta

Se planea usar el software Cobian Backup, que es un programa multitarea capaz de crear copias de seguridad en un equipo, red local o servidor. Es un programa que corre en sistemas Windows, consume pocos recursos y puede estar funcionando en segundo plano.

Se instalará el software en cada uno de los equipos, se determinarán las carpetas específicas en donde se deberán guardar todos los documentos, para facilitar el uso de Cobian, y que solo se tenga que respaldar el contenido de las carpetas seleccionadas.

3.4.3.2 Instalación

Se descarga la última versión de la herramienta Cobian Backup desde la página web oficial “www.cobiansoft.com/cobianbakup.htm”, hasta el momento se tiene la versión 11. En la Figura 12 se muestra la página de descarga del programa.

Figura 12. Página de descarga de Cobian.

Ejecutar el instalador de la herramienta.

Cambiar el lenguaje a español y dar click en la casilla “Próximo” como se muestra en la Figura 13.

Figura 13. Wizard de instalación de Cobian.

Seleccionar el recuadro “Yo acepto las condiciones” y dar click en la casilla “Próximo” como se muestra en la Figura 14.

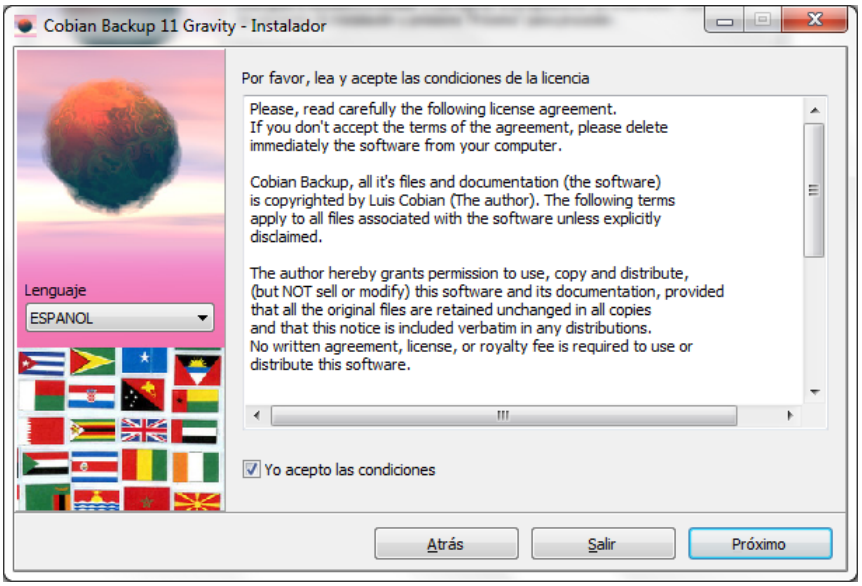


Figura 14. Wizard de instalación de Cobian.

Verificar que los recuadros “Crear íconos en el menú de inicio” e “Instalar el solicitante de Volume Shadow Copy”, y dar click en “Próximo” como se muestra en la Figura 15.

Figura 15. Wizard de instalación de Cobian.

En Tipo de instalación seleccionar “Como un servicio”.

En Opciones de servicio seleccionar “Usar como una cuenta normal”.

- Escribir el nombre del equipo en el que se está instalando la herramienta.
- Establecer una contraseña, si se cree conveniente.

Dar click en “Próximo” como se muestra en la Figura 16.

Figura 16. Wizard de instalación de Cobian.

Dar click en “Instalar” como se muestra en la figura 17.

Figura 17. Wizard de instalación de Cobian.

En la Figura 18 se muestra el progreso de la instalación del programa.

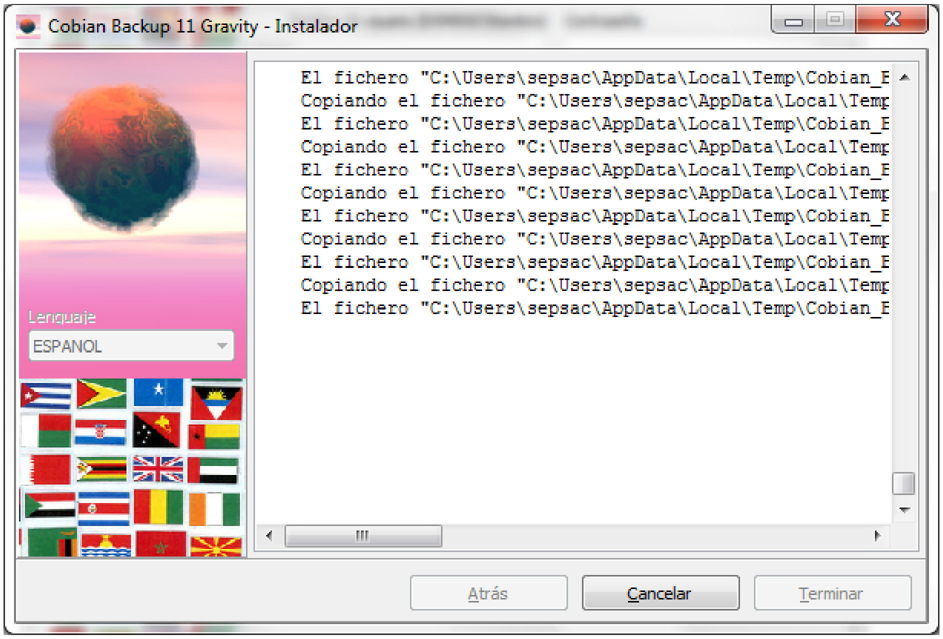


Figura 18. Wizard de instalación de Cobian.

3.4.3.3 Configuración de la tarea de respaldo

Abrir la herramienta de Cobian Backup, en la Figura 19 e muestra la ventana de inicio de Cobian.

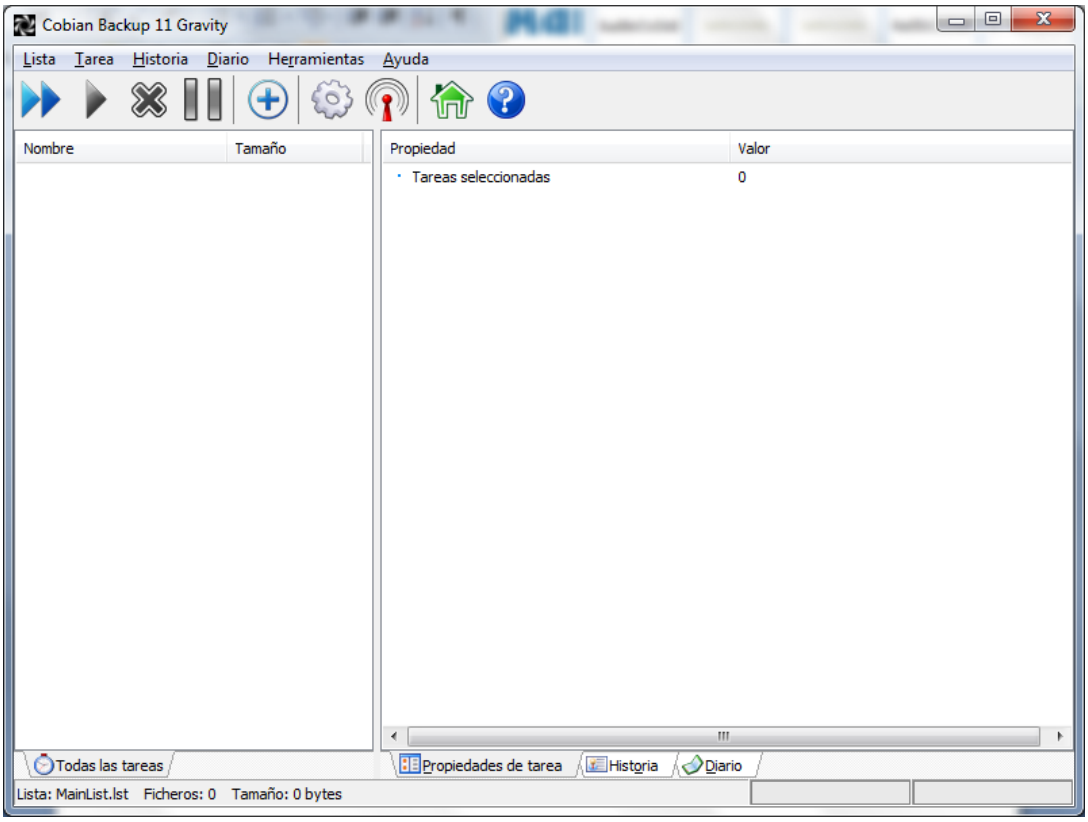


Figura 19. Interfaz de Cobian.

Dar click en “Tarea”.

- Dar click en “Nueva tarea” como se muestra en la Figura 20.

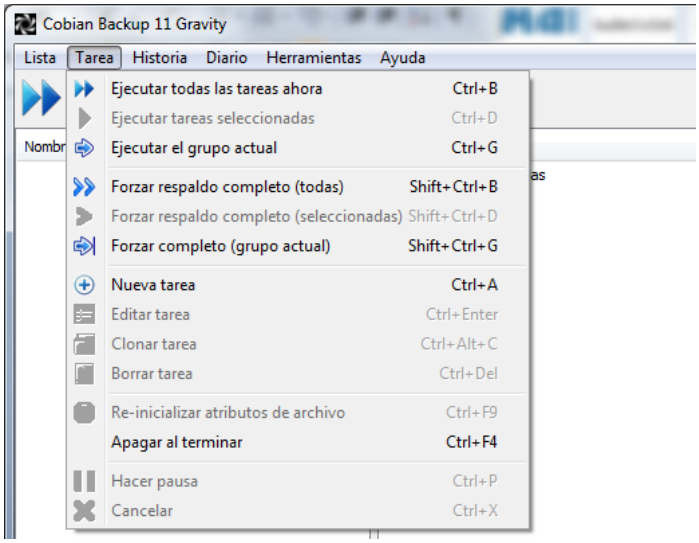


Figura 20. Tarea.

En la sección “General”:

- Dar nombre a la tarea.
- Verificar que los recuadros estén seleccionados.
- En tipo de respaldo, seleccionar “Incremental” como se muestra en la Figura 21.

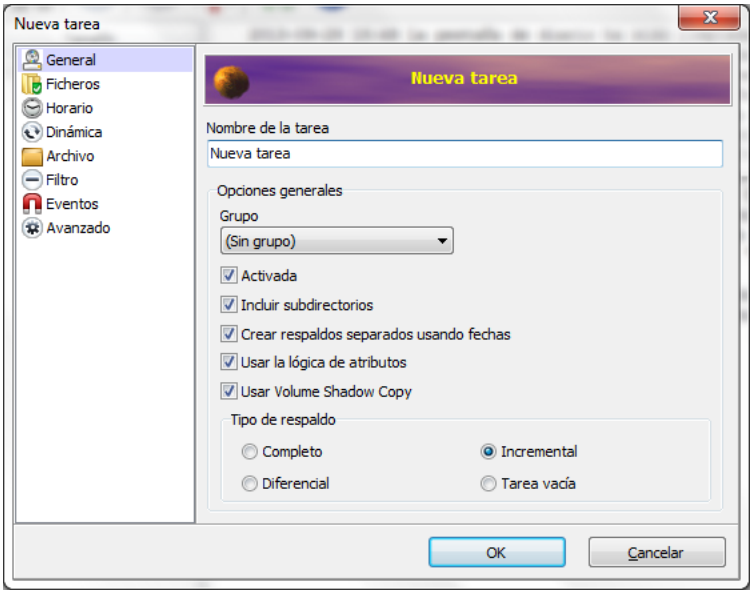


Figura 21. Nueva tarea.

En la sección “Ficheros”:

- En “Fuente”.
  - Dar click en “Agregar”.
  - Dar click en “Carpeta”.
  - Buscar y seleccionar la carpeta que se desea respaldar.
- En “Destino”.
  - Dar click en “Agregar”.
  - Dar click en “Carpeta”.
  - Buscar y seleccionar en donde se guardará el respaldo.

En la Figura 22 se muestra como se agregan los archivos a respaldar tanto en la fuente como en el destino.

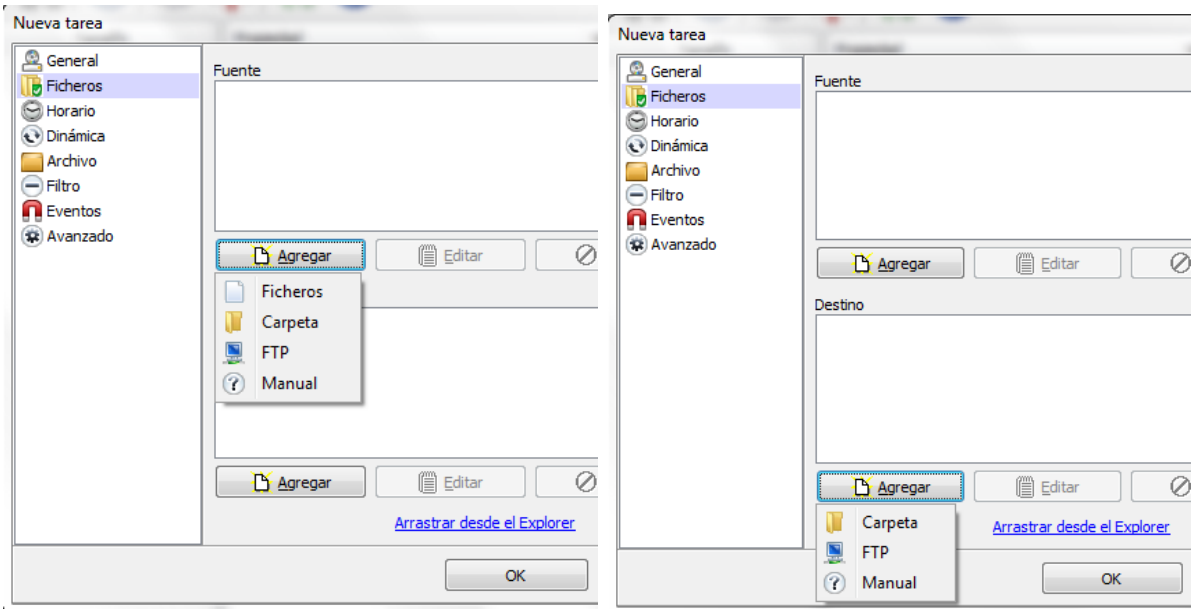


Figura 22. Agregar ficheros fuente y destino de respaldo.

La tarea ha sido creada, se puede ver la tarea en el panel de tareas y las características con la cual se configuró como se muestra en la Figura 23.

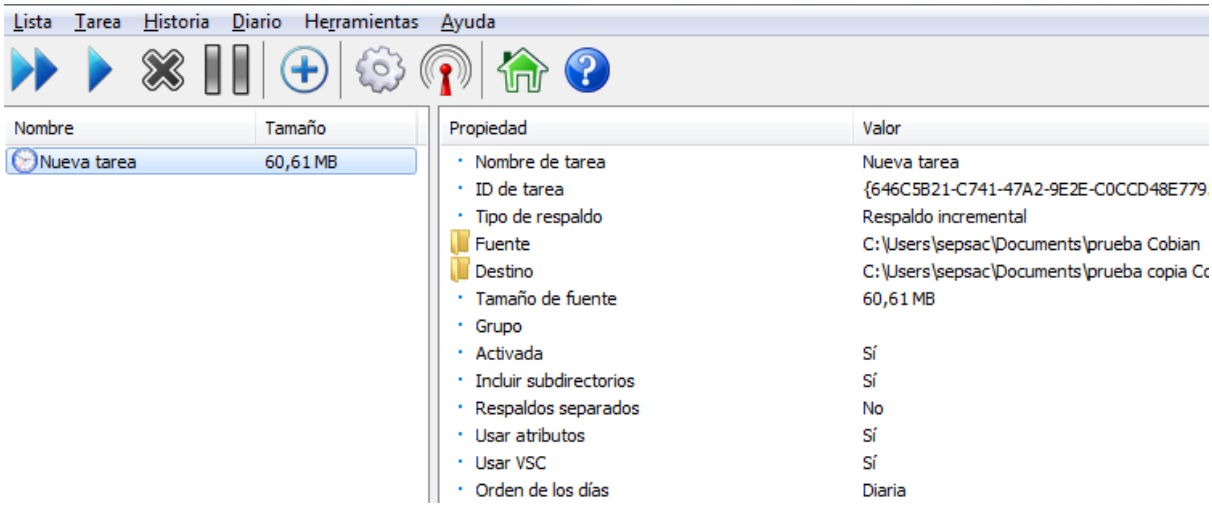


Figura 23. Nueva tarea creada.

Para realizar el respaldo se debe ejecutar la tarea:

- Dar click derecho en la tarea a ejecutar.
- Dar click en “Ejecutar tareas seleccionadas” como se muestra en la Figura 24.

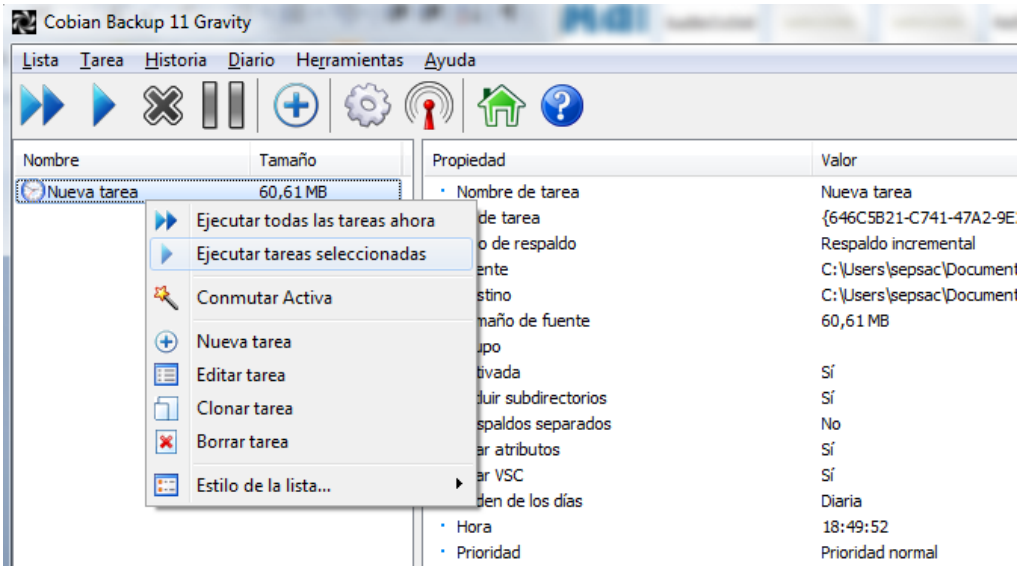


Figura 24. Ejecutar tarea.

Dar click en la casilla “Ok” como se muestra en la Figura 25.

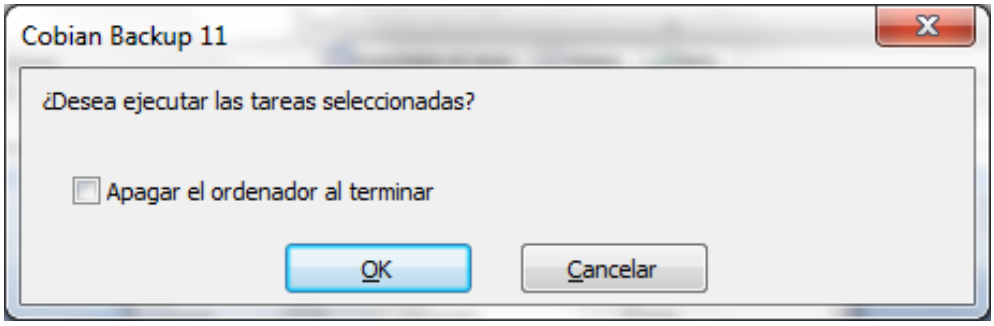


Figura 25. Confirmar ejecución de tarea.

Al ejecutar la tarea de respaldo se muestra el avance de la tarea, y un log de dicho avance, mostrando si hubo algún error. En la Figura 26 se muestra un ejemplo del resultado después de la ejecución de una tarea creada con Cobian.

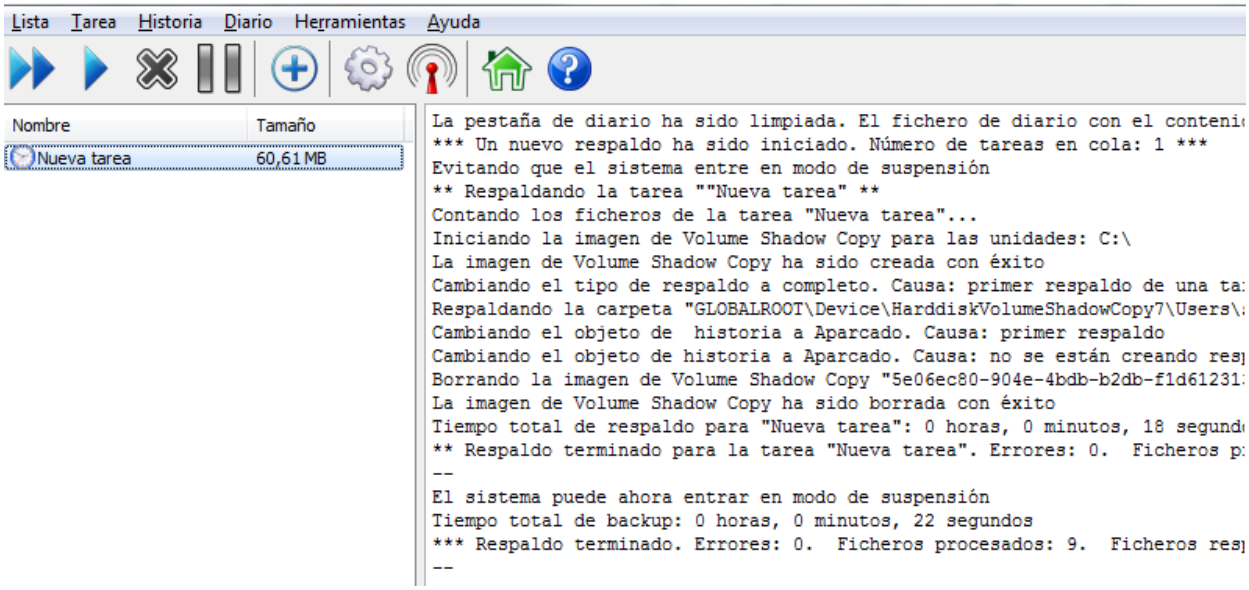


Figura 26. Resultado.

Una vez concluido este proceso, se debe asegurar que el respaldo fue hecho con éxito.

3.4.3.4 Almacenamiento Conectado en Red (NAS)

Se guardará la información en un dispositivo NAS (Network Attached Storage), es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de una computadora con computadoras personales o servidores clientes a través de una red (para más información consultar el Anexo 2).

3.4.3.5 Horario

Debido al horario laboral, tomando en cuenta la cantidad de documentos que se pueden llegar a generar cada día, y las variaciones a la hora de salida por parte de cada una de las personas, se ha determinado que se programe la elaboración de un respaldo al día, a las 6 de la tarde.

3.4.4 Configuración y Administración de los Firewalls

El 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.

Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

La empresa proporcionó un par de equipos de firewall de la marca Fortinet, dada la fiabilidad y reputación que los preceden. El objetivo de tener dos equipos, es el poder implementar la función de alta disponibilidad (HA).

La función de alta disponibilidad es una medida de seguridad necesaria para disminuir el riesgo de ver afectado el rendimiento y operatividad de la red de la empresa. Se establece el primer firewall como “maestro” y el segundo como “esclavo” como se muestra en la Figura 27, en caso de que el firewall establecido como maestro falle, el firewall esclavo se activa convirtiéndose en el dispositivo que filtra la actividad de la red.

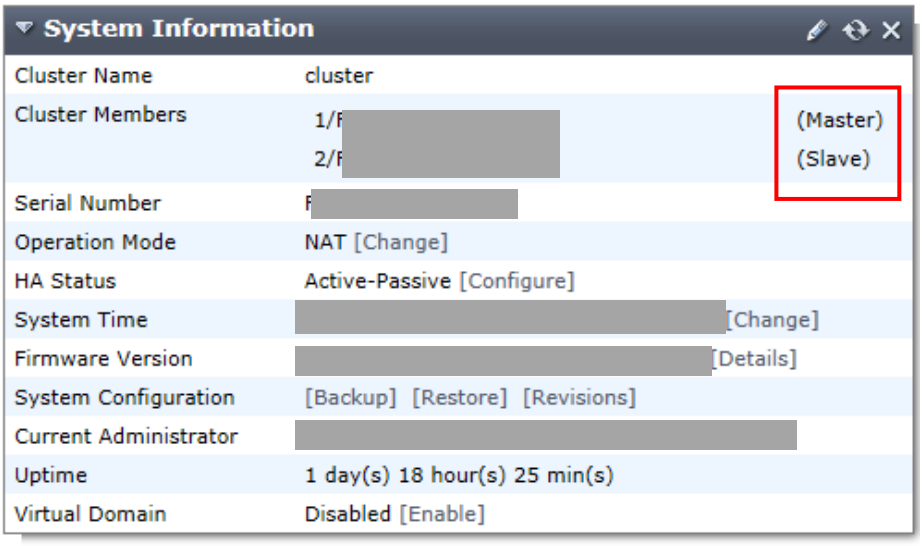


Figura 27. Información del sistema.

3.4.4.1 Interfaces

El firewall nos permite configurar las diferentes interfaces de una manera relativamente sencilla, para configurar la función de alta disponibilidad se debe establecer las diferentes interfaces manualmente, para lo cual se debe tener el conocimiento de la estructura de red con la que se está trabajando.

Durante el desarrollo del proyecto se me encargó la responsabilidad de llevar un control de la red, y de saber el papel que lleva a cabo cada dispositivo que la compone. En la Figura 28 se muestran las diferentes interfaces que maneja cada firewall.

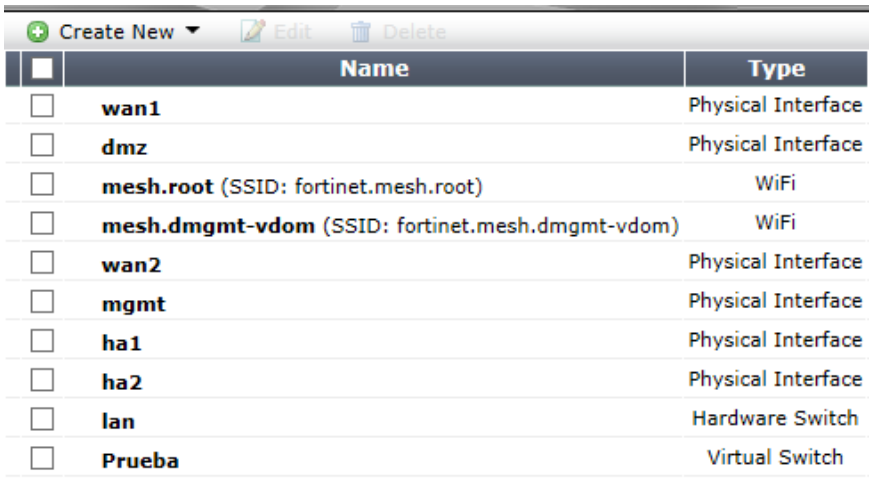


Figura 28. Interfaces.

El firewall permite crear una nueva interfaz como en la Figura 29, que se puede configurar como interfaz de tipo VLAN (Virtual Local Area Network), definir la dirección IP que va a tener la interfaz que se está creando, el acceso que se puede tener, etc., que se pueden configurar de acuerdo con las necesidades que se tengan.

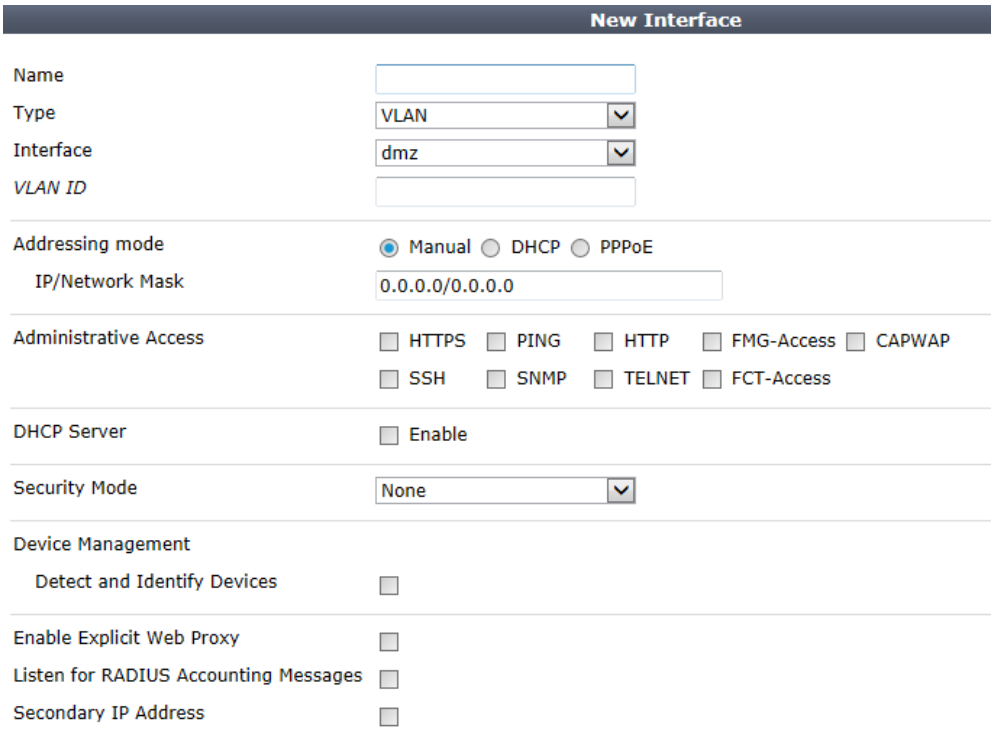


Figura 29. Creación de una nueva interfaz.

3.4.4.2 Ruta de salida

Se debe configurar la ruta de salida de la red interna hacia el exterior, por lo que se configura el gateway con la dirección que será la puerta de enlace, que es la dirección que podemos ver en los equipos de cómputo pertenecientes a la red interna. En la Figura 30 se presenta el despliegue de la ruta de salida.

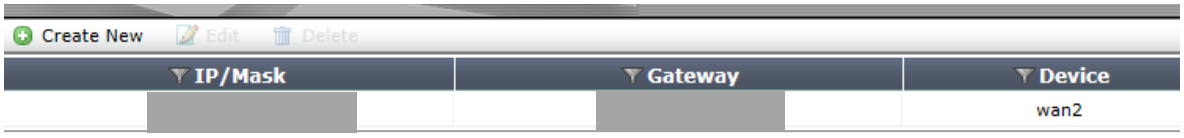


Figura 30. Ruta de salida.

Se puede configurar o crear una nueva ruta estática como en la Figura 31, se define la dirección IP y la máscara de red que tendrá, la interfaz que será la que usará la ruta estática, la puerta de enlace, también permitiendo configurar los valores de distancia y prioridad de la conexión.

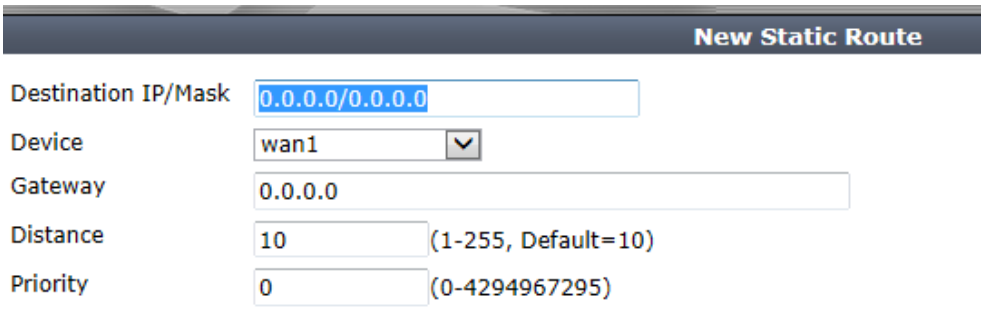


Figura 31. Creación de una nueva ruta.

3.4.4.3 Reglas

Hay dos filosofías básicas en la configuración de un firewall, permisiva o restrictiva, en el caso de los dispositivos de trabajo se presenta una política restrictiva, es decir, todo lo que no esté permitido está prohibido.

Las reglas se pueden crear, eliminar o modificar como en la Figura 32 de acuerdo con las necesidades de la empresa, estableciendo un orden jerárquico, es decir, las reglas más particulares deben establecerse al inicio y las más genéricas deben establecerse al final, ya que si se hace de manera inversa puede llegar a negarse una comunicación muy específica que una regla particular sí permite, pero al estar una regla genérica antes la conexión no se permite.

Se debe conocer el sentido de las comunicaciones antes de establecer las reglas, existen dos direcciones, desde la red interna a la red externa y de la red externa a la red interna. En la comunicación de adentro hacia afuera se deben establecer las reglas que especifiquen qué equipos, por medio de qué protocolos y si se permite o no la comunicación. En la conexión que viene desde el exterior a algún equipo de la red interna, lo que se recomienda es no permitir ninguna conexión que venga de internet. En a Figura 32 se muestra la interfaz gráfica de la administración de las reglas del firewall.

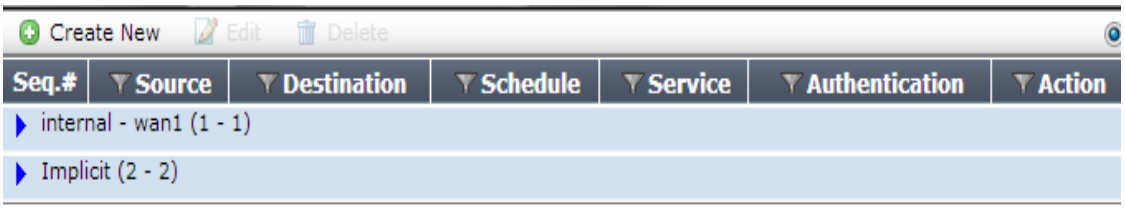


Figura 32. Reglas.

Se pueden crear tantas reglas como sean necesarias. Se permite definir el tipo y subtipo de la política que se está creando. En la Figura 33 se muestra los campos requeridos para configurar una nueva regla en el firewall.

Se configura la interfaz por la que se establece la conexión y su dirección de origen, así como la interfaz de destino y la dirección destino. En el apartado de "Direcciones" se pueden definir las direcciones a las cuales se quiere acceder, dando el valor de "ANY" se dispone que cualquier dirección o interfaz entra dentro de la política.

El horario es otro aspecto que se puede definir o bien dejar el valor "ANY", dependiendo de las características de las necesidades por las cuales se está configurando la regla. Los servicios se pueden limitar tanto como sea necesario o se crea conveniente, con la finalidad de evitar el mal uso de los recursos de red.

Por último se define si las actividades que caen dentro de las características de la política, y cuál es la acción que se desea ya sea aceptar o rechazar. En la Figura 33 se muestra la interfaz gráfica de la creación de una nueva política.

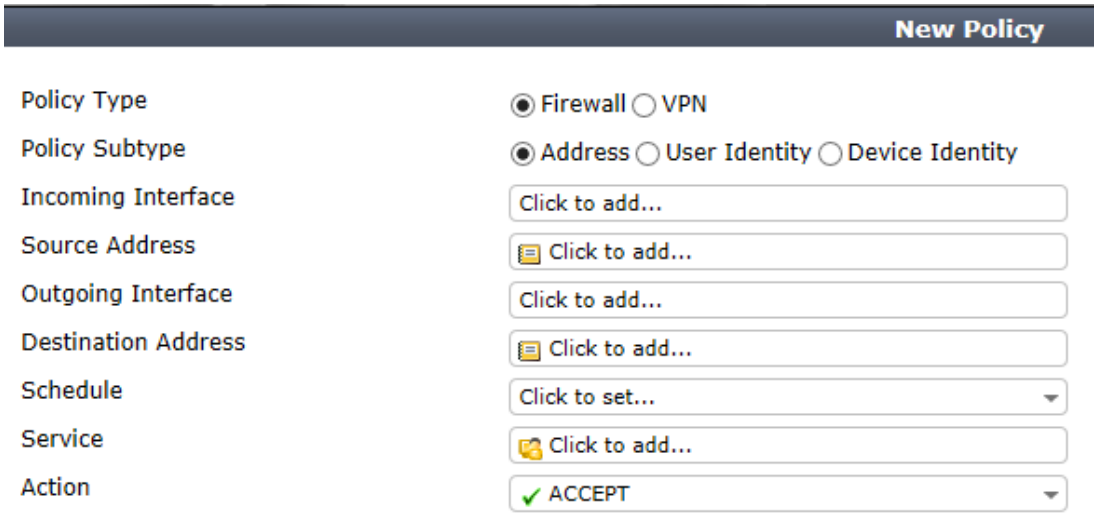


Figura 33. Creación de una nueva regla.

3.4.4.4 Direcciones

Las direcciones IP nos permiten identificar a un dispositivo en la red. En el firewall definimos diferentes grupos de redes y subredes, de acuerdo con las necesidades que se van presentando, y se definen nuevos rangos con respecto a las funciones de las diferentes áreas dentro del SOC

Por defecto se tiene configurada una subred que abarca todas las direcciones IP como se muestra en la Figura 34.

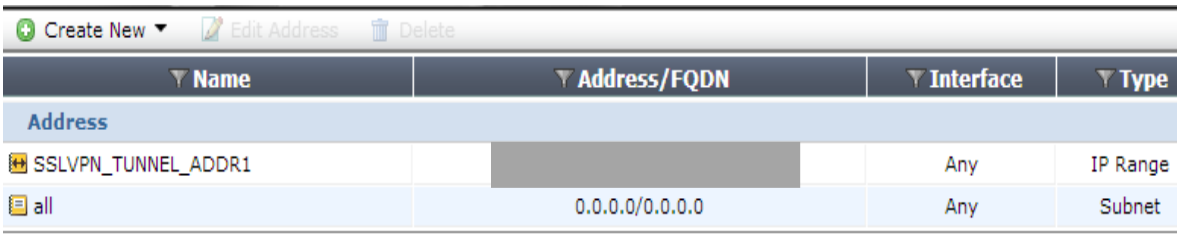


Figura 34. Direcciones.

Al configurar alguna dirección nueva se le da un nombre con el cual se pueda distinguir de las demás e indicar a qué se está haciendo referencia con ella. El tipo de la dirección permite configurar si se trata de una subred, de un rango o de una sola dirección, dependiendo del tipo, se define la dirección IP o el rango de direcciones que pertenecen a la nueva dirección. La interfaz define por dónde se comunica la nueva dirección, por último se define si se quiere mostrar con el resto de direcciones o no. En la Figura 35 se muestra la interfaz gráfica de la configuración de una nueva dirección o direccionamiento.

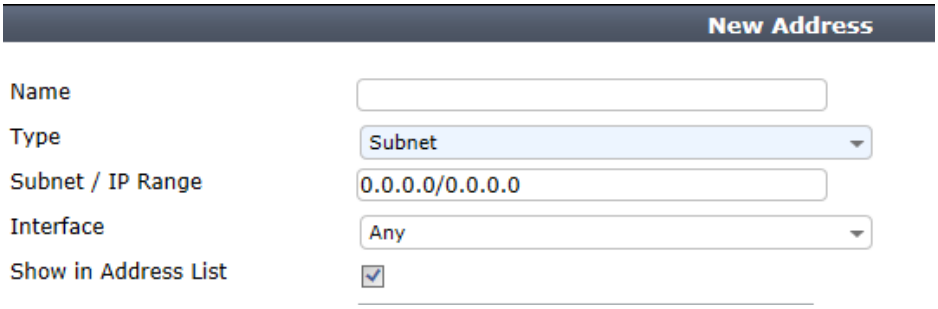


Figura 35. Creación de una nueva dirección.

3.4.4.5 Alta Disponibilidad (HA)

La función de alta disponibilidad permite configurar el conjunto de Firewalls, con los que se cuenta, formando un cluster. Alta disponibilidad es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional, durante algún evento por el cual el firewall "maestro" queda inhabilitado, ya sea por falla de hardware, software, falla eléctrica o malware, el firewall "esclavo" entra en acción y toma las funciones del maestro.

Para hacer la configuración se establece el modo de operación, el modo “standalone” se refiere a que cada firewall funciona y trabaja por su cuenta, en el modo “activo-pasivo” uno de los firewall asume la carga y en caso de caída se traspasa al otro firewall, en el modo “activo-activo” los firewalls reciben parte de la carga. Dadas las necesidades del trabajo se optó por la configuración “activo-pasivo”, para asegurar la fluidez del servicio de firewall.

Se define el nombre del conjunto que conforman los firewalls, así como un password para acceder. Se configuran las interfaces por las cuales se tiene la conectividad entre dispositivos, para así permitir la función de alta disponibilidad, y la prioridad que tiene dicha conectividad. En la Figura 36 se muestra la pantalla de configuración de alta disponibilidad.

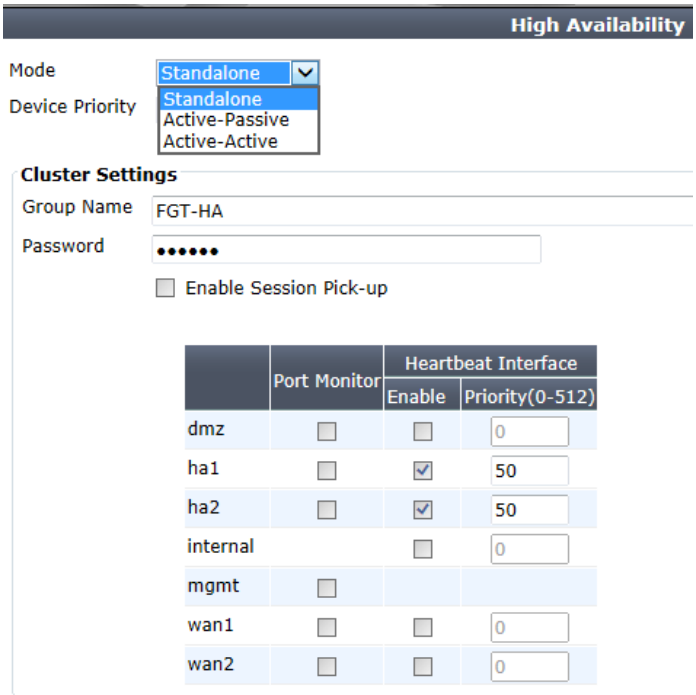


Figura 36. Configuración de alta disponibilidad.

Una vez configurada la alta disponibilidad, la interfaz cambia, desplegando una figura que representa a los firewalls, y la interfaz por la cual se encuentran comunicados entre sí como se muestra en la Figura 37.

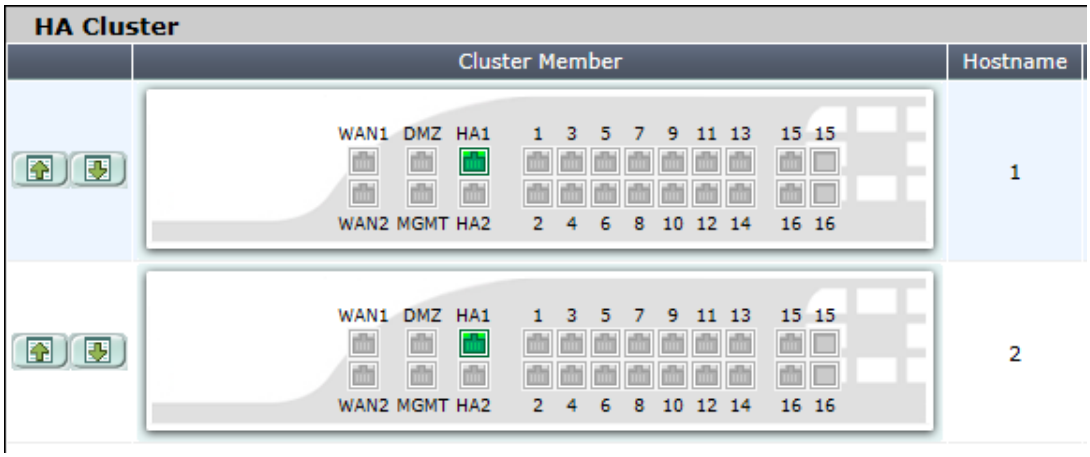


Figura 37. Clúster con alta disponibilidad.

3.4.5 “Endurecimiento” de los Firewalls

El “hardeninig” es la práctica de asegurar los sistemas reduciendo las vulnerabilidades. El propósito de este procedimiento es tener una lista de las características del firewall, así como de las configuraciones con las que se cuenta y las acciones a realizar con el fin de lograr un mayor nivel de seguridad. La auditoría se realizó con base en el documento **“Auditing fortigate firewall appliance”** que fue proporcionado por el Director del departamento Quality Assurance.

La secuencia del número de las tablas puede no ser continuo debido a que la información contenida en las tablas faltantes se consideró de carácter sensible para la empresa, por el mismo motivo algunos datos contenidos en las tablas fueron modificados.

3.4.5.1 Tablas

Tablas con información específica de las configuraciones, necesidades y funciones de los Firewalls.

3.4.5.1.1 Procesos de negocio claves que se basan en la disponibilidad del firewall

En la Tabla 1 se muestran los principales procesos de negocio de la compañia, estos elementos se consideran de mayor importancia para el desarrollo de las activdades de cada departamento.

Tabla 1 Procesos de negocios.

Proceso de negocio 1	Internet
Proceso de negocio 2	Monitoreo
Proceso de negocio 3	VPN
Proceso de negocio 4	Correo electrónico
Proceso de negocio 5	Documentos

3.4.5.1.2 Requerimientos de integridad, confidencialidad y disponibilidad

En la Tabla 2 se presenta el valor que tiene cada uno de los procesos de negocio con respecto a los pilares de la seguridad de la información (integridad, disponibilidad y confidencialidad).

Tabla 2 Requerimientos de Procesos.

#	Procesos de negocio claves o Funciones de negocio soportadas por Fortigate	Integridad (Valor de impacto)	Confidencialidad (Valor de impacto)	Disponibilidad (Valor de impacto)
1	Internet	Medio	Medio	Alto
2	Monitoreo	Alto	Medio	Alto
3	VPN	Medio	Medio	Alto
4	Correo electrónico	Alto	Alto	Alto
5	Documentos	Alto	Alto	Alto

3.4.5.1.3 Riesgos identificados

En la Tabla 3 se identifican los riesgos que corren los activos de la empresa y las vulnerabilidades que podrían explotarse.

Tabla 3 Riesgos identificados.

#	Vulnerabilidad/Exposición	Riesgo	Activos afectados
1	Ajustes del Firewall por default	• Servicios peligrosos y desconocidos que pasan libremente • Podrían servir	• Datos personales • Documentos • Inventarios • Correo electrónico • Computadoras

		como participantes de una denegación de servicios • Login de agentes hostiles o usuarios sin autorización • Exposición de información sensible a usuarios escuchando sin autorización • Address spoofing • Ataques de Overflow o ataques de DoS (Denegación de Servicio) • Terceras partes maliciosas podrían ganar acceso a aplicaciones críticas	• Servidores
2	Mal configuración del Firewall	• Servicios peligrosos y desconocidos que pasan libremente • Podrían servir como participantes de una denegación de servicios • Login de agentes hostiles o usuarios sin autorización • Ataques de Overflow o ataques de DoS(Denegation of Service). • Terceras partes	• Datos personales • Documentos • Inventarios • Correo electrónico • Computadoras • Servidores

		maliciosas podrían ganar acceso a aplicaciones críticas • Administración centralizada • Puertos abiertos • Alta disponibilidad deshabilitada	
3	Malware	• Pérdida de información • Pérdida de secretos • Incremento en el costo de la recuperación (tiempo, recursos) • Pérdida de reputación	• Datos personales • Documentos • Computadoras • Servidores • Ancho de banda • Conectividad • Correo electrónico
4	Proveedor de Servicio de Internet	• Pérdida de acceso a internet • Conexión lenta	• Ancho de banda • Correo electrónico

3.4.5.2 Auditoría de Checklist

Comprobar los elementos de un proceso de auditoría, con el siguiente proceso se marca el estado de una lista de artículos sobre las configuraciones en el firewall, en caso de no contarse con la característica mencionada se marca la casilla "**N/A**", en caso de que se cumpla se marca la casilla "**Pasa**" y en caso de que no se cumpla se marca la casilla "**Falla**".

3.4.5.2.1 Acceso y configuración / cambio de Administración

En la Tabla 4 se revisa si se cuenta con dos configuraciones de administración del firewall.

Tabla 4 Elementos de auditoría.

N/A	Pasa	Falla	#	Comprobar elemento de la lista	Riesgo
	X b)	X a)	1	a) Sólo el administrador del Firewall y otro personal autorizado pueden tener acceso a la administración del firewall b) El Firewall deben ser administrado desde un host confiable	Alto
Riesgo de no cumplirse		Acceso a usuarios no autorizados y hosts inseguros dejan el firewall susceptible a que intrusos modifiquen las reglas del firewall, corrompa su integridad y niega la disponibilidad a usuarios legítimos.			
Procedimiento		Conectarse a la interfaz interna del firewall usando el cliente de SSH. En la interfaz de línea de comandos (CLI) ingresar como administrador y ejecutar los comandos necesarios.			
Verificación		El resultado mostrará el nombre de usuario Administrador y la dirección IP específica confiable de donde se puede conectar al FW y sus permisos de lectura/escritura			

En la Tabla 5 se evalua si se tiene configurado la terminación de una sesión en la interfaz del firewall, después de transcurrido un tiempo determinado sin que se haya realizado algun movimiento en dicha interfaz.

Tabla 5 Periodo de tiempo fuera.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		3	El periodo de tiempo-fuera para una consola desatendida no debe ser mayor a 15 minutos. Activando este periodo de tiempo-fuera provee de seguridad adicional	Alto
Riesgo de no cumplirse		Abuso casual o malicioso de uso a través de la sesión abierta (para periodos más largos de tiempo fuera) por usuarios desautorizados, si tienen acceso físico a la sesión.			
Procedimiento		En CLI loggear como administrador y ejecutar el siguiente comando: a) Fortigate# get system option b) Loggear y esperar por la expiración del periodo de tiempo fuera. El sistema debe forzar a iniciar sesión nuevamente			
Verificación		El valor de ‘Admin timeout’ es 5 minutos			

La Tabla 6 evalua si se tienen deshabilitadas las interfaces físicas del firewall que no se esten usando, con el fin de prevenir ataques de acceso no autorizado.

Tabla 6 Interfaces del Firewall.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
		X	5	El administrador del firewall deshabilitará las interfaces del mismo que no estén en uso	Alto
Riesgo de no cumplirse	Ataques de escaneo y spoofing, intentos de acceso no autorizado al firewall a través de redes no confiables. Si es exitoso, habilita una puerta trasera al firewall y a la red interna para el intruso				
Procedimiento	En la CLI ejecutar el siguiente comando: Fortigate # get system interface				
Verificación	Se muestra la lista de interfaces levantadas. Asegurar que la interfaz DMZ está deshabilitada				

La Tabla 7 evalúa que las interfaces de administración se encuentren debidamente restringidos.

Tabla 7 Acceso administrativo.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		6	Asegurar que solo los puertos de la interfaz interna serán usados para acceso administrativo al firewall y están restringidos a cifrados SSH o SSL	Alto
Riesgo de no cumplirse	Ataque del “hombre en medio”, sesión de hijacking				
Procedimiento	En la CLI ejecutar el siguiente comando: a) Fortigate# get system interface b) Intenta ingresar a la interfaz externa a través de la interfaz web o usando putty				
Verificación	Revisar si la línea “Access:” lee ‘ssh, https’ solo para la interfaz interna. No debería ser capaz de ingresar a la interfaz externa del firewall				

En la Tabla 8 se comprueba que cualquier acceso administrativo crea un registro (log) del evento.

Tabla 8 Logs de acceso administrativo.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		7	El administrador del firewall se asegurará que para todos los accesos administrativos y modificaciones en la configuración del firewall se crean registros	Alto
Riesgo de no cumplirse	Violaciones de acceso sin detectar al firewall y cambios en la configuración de ajustes del firewall				
Procedimiento	En la interfaz web accede como administrador: a) Seleccionar Log & Report -> Log setting -> Config Policy				

	b) Seleccionar HA activity event y después ok. Desmarcar “HA activity event” y después elegir “ok”
Verificación	a) Verifica que dentro de Log & Report -> Log Setting -> config Policy -> Event Log: ‘admin login/logout event’ y ‘when configuration has changed’ son seleccionados. b) Revisar los logs para verificar que los cambios en las políticas de logs son grabados

La Tabla 9 revisa si se tienen respaldos de las configuraciones.

Tabla 9 Respaldos de configuración.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		8	La configuración previa y actual del router se hacen respaldos y salvados en una ubicación segura	Alto
Riesgo de no cumplirse	Cambios sin autorización en la configuración y corrupción de los archivos almacenados. Sin protección de Backup afecta el Real-time Recovery Objective (RTO)				
Procedimiento	a) Pedir al administrador que muestre la ubicación de los archivos de respaldo de configuración. b) Crear un nuevo respaldo y almacenarlo en el mismo directorio				
Verificación	Revisar las fechas de creación de los archivos de configuración. Deben ser diferentes. Revisar si los archivos son almacenados en un sistema seguro.				

En la Tabla 10 se revisa que los archivos de respaldo de configuración del firewall se encuentren en una ubicación dentro de un sistema operativo el cual es usado para restringir el acceso a dichos archivo.

Tabla 10 Seguridad de sistema operativo local.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
X			9	En el sistema en donde los archivos de configuración son guardados, los mecanismos de seguridad del sistema operativo local serán usados para restringir el acceso a los archivos	Alto
Riesgo de no cumplirse	Cambios sin autorización en la configuración y corrupción de los archivos almacenados. Sin protección de Backup afecta el Real-time Recovery Objective (RTO)				
Procedimiento	Pedir al administrador que muestre la ubicación de los archivos de respaldo de configuración. Comparar los permisos de seguridad de los archivos de respaldo de configuración viejo y nuevo.				
Verificación	Revisar si el folder está localizado en un dispositivo con formato				

	NTFS. Revisar las propiedades de seguridad del folder. Verificar que solamente el administrador del firewall todos los permisos del folder

La Tabla 11 se centra en la descarga de los parches y las actualizaciones desde los sitios oficiales Fortinet.

Tabla 11 Últimos parches y actualizaciones.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		10	Asegurar que los últimos parches y actualizaciones son aplicados a los componentes del firewall. Si los parches y actualizaciones son descargados automáticamente de las páginas web de los vendedores, asegurar que la actualización es recibida desde un sitio confiable	Alto
Riesgo de no cumplirse		Explotación de vulnerabilidades conocidas			
Procedimiento		a) Usa la interfaz web e ingresa como administrador. Nota el firmware, antivirus y versiones de definiciones de ataques b) Preguntar al administrador ingresar al sitio de soporte de Fortinet y mostrar las últimas versiones de estos artículos c) Revisar si la función de actualización automática			
Verificación		Compara los números de versión. Las versiones en Fortigate deben ser las más recientes			

En la Tabla 12 se revisa que se tienen configuradas reglas “básicas” para la protección de la red local de conexiones provenientes del exterior en el firewall.

Tabla 12 Reglas de exterior a interior.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		11	Revisar las reglas del exterior al interior para asegurar que siguen el siguiente orden: • Bloqueo del firewall • Filtros anti-spoofing (direcciones privadas bloqueadas, direcciones internas apareciendo desde afuera) • Negar servicios entrantes no deseados • Reglas de permisos de usuarios	Alto

				• Negar y alertar (alertar al administrador de sistemas sobre el tráfico sospechoso) • Negar y crear logs (loggear el tráfico restante para su análisis) Los firewalls operan con base en la primera igualdad, así la estructura de arriba es importante para asegurar que el tráfico sospechoso se mantenga fuera en lugar de permitirle acceso inadvertidamente por no seguir el orden apropiado	
Riesgo de no cumplirse	Malas configuraciones. Reglas establecidas inefectivas				
Procedimiento	Ingresar como administrador usando la interfaz web. a) Seleccionar Firewall -> Addresses -> External b) Seleccionar Firewall -> Policy -> 'EXT>INT'				
Verificación	Revisar el orden de las reglas				

En la Tabla 13 se revisa que se tengan las reglas necearias para permitir las conexiones desde el interior hacia el exterior de la red.

Tabla 13 Reglas de interior a exterior.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		12	Revisar las reglas del interior al exterior para asegurar que siguen el siguiente orden: • Permitir el túnel ipsec • Filtros anti-spoofing (direcciones privadas bloqueadas, direcciones internas apareciendo desde afuera) • Bloquear servicios salientes no deseados • Reglas de permisos de usuarios • Negar y crear logs (loggear el tráfico restante para su análisis) Los firewalls operan en base al primer match, así la estructura de arriba es importante para asegurar que el tráfico	Alto

				sospechoso se mantenga fuera en lugar de permitirle acceso inadvertidamente por no seguir el orden apropiado	
Riesgo de no cumplirse	Malas configuraciones. Reglas establecidas inefectivas				
Procedimiento	Ingresar como administrador usando la interfaz web. a) Seleccionar Firewall -> Addresses -> Internal b) Seleccionar Firewall -> Policy -> 'INT>EXT'				
Verificación	Revisar el orden de las reglas				

En la Tabla 14 se revisa si se tienen configurados los protocolos que se deben rechazar para evitar posibles ataques.

Tabla 14 Rechazo de protocolos.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
		X	13	Rechaza los siguientes protocolos riesgosos y servicios en cualquier dirección	Alto

Puerto (Transporte)	Servicio	
1 (TCP / UDP)	tcpmux	
7 (TCP / UDP)	echo	
9 (TCP / UDP)	Discard	
11 (TCP)	Systal	
13 (TCP / UDP)	Daytime	
15 (TCP)	Netstat	
19 (TCP / UDP)	Chargen	
67 (UDP)	Bootp	
69 (UDP)	Tftp	
135 (TCP / UDP)	Loc-srv	
137 (TCP / UDP)	Netbios-ns	
138 (TCP / UDP)	Netbios-dgm	
139 (TCP / UDP)	Netbios-ssn	
177 (UDP)	Xdmcp	
445 (TCP)	Netbios (ds)	
512 (TCP)	Rexec	
515 (TCP)	Lpr	
517 (UDP)	Talk	
518 (UDP)	Ntalk	
540 (TCP)	Uucp	
1900, 5000 (TCP / UDP)	Microsoft UPnP SSDP	
12345 (TCP)	NetBus	
12346 (TCP)	NetBus	
31337 (TCP /	Back Orifice	

			UDP)		
Riesgo de no cumplirse	Estos puertos pueden ser usados para denegaciones de servicio y/o envío de código malicioso				
Procedimiento	Ingresar como administrador a la interfaz web. Seleccionar Firewall -> Service -> Custom Los servicios personalizados son puertos/servicios adicionales que no están en la lista predefinida. Los servicios sin autorización de un grupo contienen todos los puertos que son innecesarios y entrada denegada a la red. Revisar si este grupo de servicios es negado y el acceso es habilitado en ambas políticas EXT>INT y INT>EXT				
Verificación	Verifica que la lista refleja los puertos mencionados en esta lista.				

En la tabla 15 se revisa si se tienen configurados los protocolos que se pueden aceptar en conexiones hacia el interior de la red local.

Tabla 15 Permiso de protocolos de entrada.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		14	Permitir solamente protocolos y servicios de entrada requeridos	Alto
Riesgo de no cumplirse	Los intrusos podrían explotar servicios desconocidos y no requeridos				
Procedimiento	Realiza un escaneo de puertos a la IP de la interfaz externa				
Verificación	Verificar que los puertos detectados estén correctos				

En la tabla 16 se revisa si se tienen configurados los protocolos que se pueden aceptar en conexiones hacia el exterior de la red local.

Tabla 16 Permiso de protocolos de salida.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		15	Permitir solamente protocolos y servicios de salida requeridos	Alto
Riesgo de no cumplirse	Programas maliciosos, conexiones de proxy podrían proporcionar conexiones de puertas traseras a un intruso afectando la confidencialidad y la integridad de los datos. Se convierte involuntariamente en participante de ataques de DoS				
Procedimiento	Realiza un escaneo de puertos a la IP de la interfaz interna				
Verificación	Verificar que los puertos detectados estén correctos				

En la Tabla 17 se verifica el bloqueo del protocolo ICMP en la interfaz externa del firewall.

Tabla 17 Rechazo de tráfico ICMP.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		16	Rechazar el tráfico de entrada que contenga tráfico ICMP. Revición de registros de eventos (logs)	Alto
Riesgo de no cumplirse	Los intrusos podrían recolectar información para ataques de denegación de servicios				
Procedimiento	Verificar que el protocolo ICMP 8, 11 y 3 están bloqueados en la interfaz externa. Ingresa como administrador a la interfaz web. Selecciona Firewall -> Policy -> 'EXT>INT'. Revisar si este servicio en específico está incluido en el grupo de servicios prohibidos o si por si solo aparece en las reglas establecidas y establecer a negar acceso.				
Verificación	Revisar que el servicio predefinido ICMP_Any se encuentra en la lista de servicios no permitidos				

3.4.5.3 Filtro de direcciones

La Tabla 18 revisa si se tienen filtradas las direcciones de redes externas.

Tabla 18 Rechazo de tráfico proveniente de redes externas.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		17	Rechazar todo tráfico proveniente de redes externas que tienen alguna dirección IP: 0.0.0.0/8 Broadcast histórico 10.0.0.0/8 RFC 1918 red privada 169.254.0.0/16 Link redes locales 172.16.0.0/12 RFC 1918 red privada 192.168.0.0/16 RFC 1918 red privada 224.0.0.0/4 Multicast clase D 240.0.0.0/5 Reservado Clase E 248.0.0.0/5 Sin asignar 255.255.255.255/32 Broadcast	Alto
Riesgo de no cumplirse	IP spoofing para iniciar el intento de denegación de servicio o mandar códigos maliciosos				
Procedimiento	Acceder al Firewall como administrador por la interfaz web. Seleccionar Firewall -> Policy -> 'EXT>INT'				
Verificación	Verificar que las direcciones de arriba están incluidas en la política y establecidas para denegar acceso y logs habilitados				

La Tabla 19 revisa que todo el tráfico proveniente de la red interna no tenga como dirección IP de origen una externa a la red.

Tabla 19 Rechazo de tráfico de salida de IP foránea.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		18	Rechazar todo tráfico proveniente de las redes internas que tengan alguna dirección IP que no pertenezca a la red interna (de salida)	Alto
Riesgo de no cumplirse	IP spoofing para iniciar el intento de denegación de servicio o mandar códigos maliciosos				
Procedimiento	Revisar las reglas de interior a exterior para la política específica				
Verificación	A las direcciones internas se debe permitir el acceso de salida				

En la Tabla 20 se inspecciona que la configuración del firewall sea capaz de restringir la salida de la red interna a direcciones IP que pertenezcan a un rango definido.

Tabla 20 Rechazo de tráfico de salida de IP dentro de rangos definidos.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
	X		19	Rechazar tráfico de salida desde un sistema usando una dirección fuente que está dentro de uno de los rangos de IP: 10.0.0.0/8, 172.16.0.0/16, 165.255.0.0/16	Alto
Riesgo de no cumplirse	IP spoofing para iniciar el intento de denegación de servicio o mandar códigos maliciosos				
Procedimiento	Revisar las reglas de interior a exterior para la política específica				
Verificación	Verificar que direcciones foráneas no tienen acceso Verificar los logs de las actividades negadas				

3.4.5.4 Protección de bloque de archivos

En la Tabla 21 coprueba que se tenga habilitado el filtro de contenido web, para una navegación segura por internet.

Tabla 21 Filtro de contenido.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
		X	26	El filtro de contenido debe estar habilitado en las políticas del firewall	Alto
Riesgo de no cumplirse	Virus y códigos maliciosos infectan la red interna. Algunos pueden crear conexiones de puertas traseras para los intrusos				
Procedimiento	Acceder a la interfaz web. Seleccionar Firewall -> Policy -> 'INT>EXT' -> Open (Edit) Policyid2				
Verificación	Antivirus y el filtro web deben estar habilitados y el perfil de contenido 'Strict' debe estar en uso				

La Tabla 22 reconoce si se tiene configurada la protección antivirus.

Tabla 22 Protección antivirus.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
X			27	Verificar contenidos de 'Strict Content Profile'. Esto controla cómo se comporta la protección antivirus	Alto
Riesgo de no cumplirse	Descarga de archivos infectados o programas que contienen códigos maliciosos o virus				
Procedimiento	Acceder como administrador en la interfaz web. Seleccionar Firewall -> Content Profile -> Strict				
Verificación	Todas las opciones deben estar seleccionadas para protección, exceptuando 'pass fragmented e-mails'				

La Tabla 23 se verifica si se tiene habilitado el bloqueo de los archivos para evitar amenazas potenciales.

Tabla 23 Bloqueo de archivos.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
X			28	Bloqueo de archivos debe estar habilitado para remover todos los archivos que plantean una amenaza potencial y para proporcionar la mejor protección de ataques de virus de computadoras activas	Alto
Riesgo de no cumplirse	Descarga de archivos o programas que contengan códigos maliciosos o virus				
Procedimiento	Acceder a la interfaz web como administrador. Seleccionar Antivirus -> File block				
Verificación	Solo archivos con extensiones .doc, .ppt, .xl deben desbloquearse para protocolos HTTP, FTP, IMAP, POP3, SMTP. Todas las demás extensiones deben ser bloqueadas para todos los protocolos				

En la Tabla 24 se comprueba que el bloqueo de archivos se encuentre habilitado.

Tabla 24 Funcionalidad de bloqueo de archivos.

N/A	Pass	Fail	#	Comprobar elemento de la lista	Riesgo
		X	29	Probar la funcionalidad de bloqueo de archivos	Alto
Riesgo de no cumplirse	Descarga de archivos o programas que contengan códigos maliciosos o virus				

Procedimiento	Desde cualquier computadora interna buscar http://www.winzip.com y tratar de descargar la versión de prueba de winzip.exe
Verificación	La descarga se debe bloquear con un mensaje de alerta de seguridad

Al momento de realizar la auditoría de los firewalls con la ayuda de este documento, pude apreciar de las fallas y las mejoras posibles que se pueden configurar y aplicar, así como la actualidad de mis conocimientos sobre las mejores prácticas a la hora de configurar un conjunto de firewalls.

CAPÍTULO 4:

Resultados y conclusiones

Resultados

El diseño de un plan de aseguramiento de la estructura base de los sistemas de la empresa dentro del SOC, así como el resguardo de la información generada por los diferentes integrantes del equipo de trabajo, ha cumplido con sus objetivos de manera satisfactoria y permitiendo ser el punto de partida para proyectos futuros.

La implementación de los procedimientos para la respuesta a posibles incidentes con respecto a los equipos de cómputo en caso de pérdidas dentro de los sistemas o pérdida de los mismos sistemas, se manifiesta como un elemento importante tanto para la recuperación de los sistemas como para el ahorro de tiempo en la restauración de los mismos, siendo un recurso valioso y requerido en varias ocasiones y escenarios.

Al poner en funcionamiento el proceso de los respaldos de toda la información generada por las distintas áreas y sus actividades dentro del SOC se mantiene una base de información segura, relacionado directamente con la recuperación de los sistemas al ser una opción más para recuperar información importante.

Se establecieron las medidas de seguridad necesarias para el desarrollo de las actividades cotidianas de los servicios proporcionados por la empresa, asegurando en lo posible, toda la actividad que se realiza por parte de los miembros de la empresa.

La configuración de los firewalls puede cambiar de acuerdo con las necesidades de las diferentes áreas de la empresa, con el trabajo de auditoría se han corregido algunos desperfectos o en su defecto se ha minimizado el riesgo al mínimo.

Conclusiones

El desarrollo de una estructura es complejo, pero en especial si se trata de una estructura inexistente si se tiene la libertad y la responsabilidad de tomar decisiones, que si bien siempre fueron supervisadas por personas con amplia experiencia, es importante tomar en cuenta las condiciones en que se está desarrollando el proyecto, así como las consecuencias que pueden llegar a ocurrir.

La base de la estructura desarrollada permite que las actividades dentro del SOC se desarrollen con la libertad y confianza necesaria, así como la tranquilidad de

saber que se cuenta con un sistema para respaldo y recuperación de la información, que hasta el momento ha sido aprovechado en más de una ocasión con resultados satisfactorios, por lo que se puede decir con seguridad que la metodología diseñada e implementada cumple su propósito.

La base de la seguridad en donde intervienen la administración de los firewalls y su endurecimiento, constituye el inicio de la estructura de la seguridad de la información dentro de la empresa, se aprovecha sus diversas funciones para obtener el mejor desempeño posible alrededor de las actividades que se desarrollan dentro del SOC, minimizando los riesgos en que pueden estar los activos conectados a la red.

Durante todo el proceso que conllevó el desarrollo de este proyecto, pude desarrollar otras habilidades que no había tomado mucho en cuenta, que en mi paso por las aulas de la Facultad de Ingeniería se me inculcaron las bases, por lo que considero que todas las situaciones en las que me encontré me han y me siguen ayudando en mi desarrollo profesional.

El conocimiento obtenido en las diversas asignaturas cursadas, y la interacción con los diferentes profesores que las imparten, han ampliado mi visión y percepción de mi ambiente, así como depurar mi punto de vista y mi forma de mirar las cosas y atacar los problemas. Lo cual ha sido fundamental para desempeñarme como un profesional en las áreas de **Redes y Seguridad**.

Considero que los conocimientos brindados por la Facultad de Ingeniería, así como la formación de Ingeniero, me dieron las bases suficientes para desarrollar el ejercicio de una profesión de manera satisfactoria y sobresaliente. Con la convicción de siempre seguir buscando el crecimiento personal y profesional no me queda más que agradecer por todo lo que han brindado, Muchas Gracias.

Glosario

Antivirus.- programas cuyo objetivo es detectar y/o eliminar virus informáticos.

Auditoría.- es el examen crítico y sistemático que realiza una persona o grupo de personas al sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

Backup.- en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Boot.- es el proceso que inicia el sistema operativo cuando el usuario enciende una computadora. Se encarga de la inicialización del sistema y de los dispositivos.

Cluster.- conjuntos o conglomerados de computadoras construidos mediante la utilización de hardware común y que se comportan como si fuesen una única computadora.

Dirección IP.- es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

DMZ.- zona desmilitarizada (DMZ, por sus siglas en inglés) es una red local que se ubica entre la red interna y la red externa, permite las conexiones desde el exterior de la red.

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. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Gateway.- es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

HA.- este término hace referencia a “alta disponibilidad” que asegura un cierto grado de continuidad operacional.

Hacker.- es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

Hardware.- se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible y es llamado software.

ICMP.- protocolo de mensajes de control de internet (ICMP por sus siglas en inglés), se usa para enviar mensajes de error.

Interfaz.- se utiliza para nombrar a la conexión física y funcional entre dos sistemas o dispositivos de cualquier tipo dando una comunicación entre distintos niveles.

ISO.- es un archivo donde se almacena una copia o imagen exacta de un sistema de archivos, normalmente un disco óptico. Se rige por el estándar ISO 9660 que le da nombre. Algunos de los usos más comunes incluyen la distribución de sistemas operativos, tales como sistemas GNU/Linux, BSD o Live CDs.

Live CD.- es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Login.- es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario.

Logs.- es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Máscara de red.- es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

NCHC.- es el Centro Nacional de Alto Rendimiento Coputacional (NCHC por sus siglas en inglés) de Taiwán.

Password.- o contraseña, es una forma de autenticación secreta para controlar el acceso hacia algún recurso.

PT.- se refiere al grupo encargado de realizar las actividades de hackeo ético.

QA.- se refiere al grupo encargado del aseguramiento de la calidad de una aplicación o sistema.

RTO.- Real-time Recovery Objective

SOC.- (Security Operation Center, Centro de Operaciones de Seguridad) es una unidad centralizada en una organización que se ocupa de cuestiones de seguridad, a nivel organizativo y técnico. Un SOC dentro de un edificio o instalación es una ubicación central desde donde el personal supervisa el sitio, utilizando diferentes tecnologías de proceso de datos.

Software.- el conjunto intangible de datos y programas de computadora, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

SSH.- se refiere al protocolo secure shell, sirve para acceder a equipos remotos a traves de conexiones cifradas.

SSL.- se refiere al protocolo de capa de conexión segura, permite la transmisión de información de forma segura.

TCP.- (Protocolo de Control de Transmisión) es un protocolo de comunicación orientado a conexión fiable del nivel de transporte.

UDP.- es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

VLAN.- (red de área local virtual) es un método de crear redes lógicas e independientes dentro de una misma red física.

Wizard.- es un tipo de interfaz de usuario que presenta una secuencia de cuadros de diálogo que llevan al usuario a través de una serie de pasos bien definidos. Tareas que son complejas, realizadas con poca frecuencia, o poco conocidas pueden ser más fáciles de realizar mediante un asistente.

Referencias

Referencias de libros y documentos

- Vacca, J. (2010). *Network and System Security*. Burlington: Elsevier
- Katz, M. (2013). Redes y Seguridad. Buenos Aires: Alfaomega
- SANS Institute. *IT Audit: Security Beyond the Checklist*

Glosario

- Redes de datos. (2013, 26 de octubre). *http://web.uservers.net/ayuda/soluciones/dominios/que-es-una-direccion-ip_NTk.html*. Concepto: dirección IP
- Redes de datos. (2013, 26 de octubre). *http://todo-redes.com/gateway-puerta-de-enlace.html*. Concepto: Gateway
- Redes de datos. (2013, 26 de octubre). *http://apuntesdenetworking.blogspot.mx/2011/08/concepto-de-mascara-de-red-o-subred.html*. Concepto: máscara de red
- Redes de datos. (2013, 26 de octubre). *http://www.alegsa.com.ar/Dic/cluster.php*. Concepto: cluster
- Redes de datos. (2013, 26 de octubre). *http://informacion.wordpress.com/2006/07/11/definicion-tcp/*. Concepto: TCP
- Redes de datos. (2013, 26 de octubre). *http://www.masadelante.com/faqs/udp*. Concepto: UDP
- Seguridad de la información. (2013, 29 de octubre). *http://www.microsoft.com/es-xl/security/resources/antivirus-whatis.aspx*. Concepto: antivirus

- Seguridad de la información. (2013, 29 de octubre). *http://www.adminso.es/recursos/Proyectos/PFC/PFC_Alberto.pdf*. Concepto: auditoría
- Seguridad de la información. (2013, 26 de octubre). *http://www.pergaminovirtual.com.ar/definicion/Hacker.html*. Concepto: Hacker
- Soporte técnico. (2013, 26 de octubre). *http://auditoriasi.blogspot.mx/2009/05/soc-ventajas-e-inconvenientes.html*. Concepto: SOC
- Soporte técnico. (2013, 26 de octubre). *http://windowsespanol.about.com/od/RedesYDispositivos/f/Que-Es-ISO.htm*. Concepto: iso
- Soporte técnico. (2013, 26 de octubre). *http://www.alegsa.com.ar/Dic/livecd.php*. Concepto: Live CD
- Soporte técnico. (2013, 26 de octubre). *http://definicion.de/software/*. Concepto: Software
- Soporte técnico. (2013, 26 de octubre). *http://www.alegsa.com.ar/Dic/asistente.php*. Concepto: Wizard
- Soporte técnico. (2013, 26 de octubre). *http://definicion.de/hardware/*. Concepto: Hardware
- Soporte técnico. (2013, 26 de octubre). *http://definicion.de/interfaz/*. Concepto: Interfaz
- Soporte técnico. (2013, 26 de octubre). *http://www.headways.com.mx/glosario-mercadotecnia/definicion/log-file-archivo-de-registro/*. Concepto: log
- Soporte técnico. (2013, 26 de octubre). *http://ciscofacil.webs.com/apps/blog/entries/show/1279634-vlan-redes-virtuales*. Concepto: vlan
- Soporte técnico. (2013, 26 de octubre). *http://www.informaticamoderna.com/Backup.htm*. Concepto: backup

- Soporte técnico. (2013, 26 de octubre). *http://www.alegsa.com.ar/Dic/login.php*. Concepto: login
- Soporte técnico. (2013, 26 de octubre). *http://tecnologia.glosario.net/terminos-tecnicos-internet/boot-206.html*. Concepto: boot

Anexos

Anexo 1

Actividad de un Security Operation Center.

Es un Centro de Operaciones de Seguridad el cual está compuesto de personas certificados en tecnologías y herramientas de redes y seguridad, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas vulnerabilidades, y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización.

El servicio presenta varias alternativas:

- Soluciones basadas en aplicaciones específicas.
- Gerenciamiento de IDS/ IPS (Sistemas de Detección y Prevención de Intrusos).
- Gestión de Logs y Correlación de eventos.
- Gestión de Redes Privadas Virtuales (VPN) (Site to Site y Cliente Remoto).
- Servicios de Consultoría, Auditoría y Asesoramiento.
- Servicios de Capacitación.

Al mismo tiempo se otorgan niveles de reportes disponibles para que los clientes tengan pleno conocimiento de lo que sucede con sus recursos, y aún más, tener información de intentos fallidos ante ataques desactivados o neutralizados.

Anexo 2

Network Attached Storage

Una caja NAS es un servidor de almacenamiento dedicado que incluye una cabecera NAS y unidades de disco conectadas a una red. La cabecera NAS es electrónica de control que asegura la interfaz entre la red y el almacenamiento. Un NAS básico puede utilizar una única cabecera, o compartir el almacenamiento interno por medio de múltiples cabeceras para acomodar un creciente ancho de banda.

Los sistemas NAS de tipo grupo de trabajo admiten un almacenamiento en disco de 1 TB a 2 TB (o más) con un pequeño grupo de cuatro a seis discos duros, según el modelo y las opciones seleccionadas. Los sistemas NAS de empresa pueden implantar muchos discos, alcanzando capacidades muy superiores a los 100 TB. La mayor parte de los sistemas NAS incluyen el soporte de RAID para protección de datos y pueden implantar niveles RAID comunes, entre ellos RAID 0, RAID 1, RAID 5 y RAID 6/DP. Los sistemas NAS también incluyen algo de RAM para usarlo de caché de los datos de red a o desde los discos.

En la práctica, una caja NAS se tiene que conectar a red de área local, por lo que la interfaz de red también es importante. Los puertos Internet Gigabit (GigE) son casi universales. Algunos productos NAS proporcionan múltiples conexiones Internet para agregar interfaces de red, o con fines de redundancia o de recuperación de fallos.

Aunque las cajas NAS suelen funcionar de modo independiente, también se pueden agrupar en clusters. Los clusters NAS, cuyo principio de funcionamiento es similar al de la informática en cluster, aparecen ante la red de área local como un único dispositivo NAS. Cada elemento incluido en el cluster puede compartir la carga de datos, y cada caja del cluster puede sustituir a otra caja que falle, mejorando el rendimiento del almacenamiento y consiguiendo una mayor disponibilidad de los soportes.

Gestión de NAS

Los dispositivos NAS suelen ejecutar su propio sistema operativo específico, y se administran y configuran mediante utilidades de software integradas que se

ejecutan en cualquier Explorador de red. Esto permite a los administradores de almacenamiento comprobar la situación del NAS, diagnosticar problemas de rendimiento e introducir cambios en la configuración del NAS desde cualquier puesto de trabajo conectado a la red de área local. Cualquier utilidad de administración debe incluir el soporte de las cajas NAS en su red de área local y debe presentar información detallada a través de una única consola.