"Responsabilidad con pensamiento positivo"

UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACION

CARRERA: FACULTAD DE SISTEMAS INFORMÁTICOS

TEMA: SISTEMA DE CONTROL Y SEGURIDAD ENDIAN FIREWALL PARA LA EMPRESA FRADA SPORT.

AUTOR: JUAN JACOB BUENO ROSALES.

TUTOR: ING. CRISTÓBAL ÁLVAREZ. DSD

AÑO: 2013

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Cristóbal Álvarez, certifico que el señor Juan Jacob Bueno Rosales con C.C, No. 0105088173 realizó la presente tesis con el título "Sistema de Control y Seguridad Endian firewall para la empresa Frada Sport", y que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Cristóbal Alberto Álvarez Abril DsD.

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, JUAN JACOB BUENO ROSALES, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

_____

Juan Jacob Bueno Rosales

C.I. 0105088173

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

El documento de tesis con título “Sistema de Control y Seguridad Endian firewall para la empresa Frada Sport, ha sido desarrollado por Juan Jacob Bueno Rosales con C.C. No. 0105088173, persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Juan Jacob Bueno Rosales

Dedicatoria

Primeramente a Dios, por encaminarte a uno de mis metas propuestas, A mis padres, porque creyeron en mí, a María José, por darme fuerzas y ánimos para emprender el éxito. Dándome ejemplos dignos de superación y entrega, Hoy puedo ver alcanzada una de mis metas gracias a ustedes.

Agradecimiento

Este proceso de titulación, es el resultado del esfuerzo conjunto de todos los que Formamos el grupo de trabajo de la Universidad Israel. Principalmente a Dios que ha puesto en mi camino el apoyo de mis padres.

Y el agradecimiento incondicional. Al Ing. Álvarez por su Paciencia y colaboración en la realización de esta tesis.

Resumen

Los niveles de vulnerabilidad e importancia de toda la información de la empresa, a través de la red global de datos, orienta procesos o mecanismos de seguridad, únicos centralizados, y segmentados en la empresa Frada Sport.

Constituye una parte fundamental para la empresa, ya que no solo corresponde a la herramienta de seguridad como tal, sino a representar gráficamente, sistemáticamente, procesos y modelos de desarrollo actuales, mediante la implementación de un sistema único de seguridad, que a más de brindar soluciones de seguridad, estructura y establece medios de estabilidad, vigilancia, modelos de desarrollo, altamente disponible e inteligentes, control organizativo y fundamental, entre otros.

Teniendo en cuenta toda la infraestructura de la red, se realiza un diseño de la red y se levanta la información de los procesos o modelos actuales, para posteriormente brindar soporte a soluciones especificas orientadas al control mayor y seguridad.

La herramienta de seguridad y control Endian Firewall, es un sistema único open source, específicamente estructurado como bitácora, capaz de brindar soluciones óptimas a la red de datos, captando y estabilizando mejores formas gráficas de control organizativo en la red de datos.

Summary

The levels of vulnerability and importance of all the information of the company through the global data network, directs security processes or mechanisms, unique centralized and segmented in the company Frada Sport.

It is a key part of the company, as it not only corresponds to the safety tool as such, but to graph systematically process and development models, by implementing a unique system security, which in addition to offering security solutions, provides media structure and stability, security, development models, highly available, intelligent, and fundamental organizational control, among others.

Considering the entire network infrastructure, makes the design of the network and information stands or current models processes, later providing specific solutions supports more control oriented and safety.

The security and control tool Endian Firewall, is a unique open source, specifically structured as records, able to provide optimal solutions to the data network, capturing and stabilizing best graphic forms of organizational control in the data network.

Tabla de Contenidos

Lista de Manual de Procesos

CAPITULO 1

2. Anteproyecto

2.1 Planteamiento del problema

Uno de los puntos principales, que se considera negativo para la empresa, es referente al personal, mencionados empleados, han ingresado a ciertas páginas de internet, lo cual contiene información o contenido malicioso, es decir, sin ningún cocimiento del uso correcto de internet identificando riesgos, destacando la presencia de virus, troyanos, corro spam, entre otros. Es así, que en innumerables situaciones dadas en la empresa, los daños se ha manifestado en el rendimiento de los equipos.

Simplemente con descargarse algún el tipo de archivo o programa de su conveniencia, de igual manera, han infectado de virus, daños en los equipos, etc, por lo que la empresa frada sport, no tiene un control centralizado de antivirus ni motor de anti- spam, o filtro que ayude a tener un mayor control a la hora de prevención de riesgos.

Los daños en “dichos equipos”, tomando en cuenta toda la infra estructura física pero sobre todo lógica de la red que implementa la empresa, ha sido afectada en el rendimiento de los mismo, perjudicando al sistema como tal, al hardware y al software que maneja la empresa, brindando problemas de nuevamente reinstalar las maquinas afectadas, perdiendo el tiempo o reduciendo las horas o la productividad de trabajo y más aun, referente a costos para cada equipos, cuando se presentan todas las eventualidades maliciosas producto de no tener el control o política de seguridad para cada usuario.

Los usuarios sin mucha experiencia en informática o seguridad pueden sentirse incómodos gestionando con las solicitudes y alertas que causen daños al quipo como contenido de publicidad, pornografía, o páginas inseguras.

También cabe recalcar, que para la empresa, es de importancia el uso de un control y organización de seguridad, por los procesos que maneja mencionada empresa, son de extrema confidencialidad y de sumo cuidado, debido a que se manejan negocios por internet, con proveedores, con bancos, con estados de cuenta, con transacciones, entre otros. Ante esto, se presenta la necesidad que dicha información sea vulnerable ante la modernización que hoy en día se conoce como hackers.

Decir también que no existe un control organizativo que permita al administrador de la red, obtener una inspección sobre cómo pasan los datos de red, una estadística de interfaces de cada máquina, graficas del sistema de cada usuario de memoria, tiempo de acceso, uso de disco, de memoria etc. Además, contar con un registro de flujo de datos de Ips, dominios, nombre de máquina, subred, etc, lo que causa problemas a la hora de instalar nuevas maquinas a la duplicidad de equipos de flujo de información de la red, y a la hora de realizar una auditoría informática.

También no existe un control de prevención de "virus, spam o correo basura", que se pueda prevenir mediante un firewall, decir también que no hay en la administración de la red, graficas de saturación o tráfico en el internet, es decir, medir las conexiones entrantes y salientes de toda la red en general, destacando su uso en la red.

En ocasiones el internet se va, se corta el flujo de datos, usuarios como tal se descargan archivos, manejan contenido web altamente dinámicas por el gran contenido de multimedia, lo que provoca demasiada lentitud y fallas en la red.

Definición del problema de investigación

El principal problema que la empresa Frada Sport posee, es la de no contar con un sistema de control y seguridad, un sistema que le permita a cada usuario de la empresa ser controlado a nivel de restricción de páginas de internet, por ejemplo que no están autorizados, es decir un bodeguero no debe tener acceso a internet, sino netamente lo laboral, a diferencia de un empleado del área de contabilidad que debe tener acceso a ciertas páginas de internet pero restringidas algunas.

2.2 Delimitación del problema de investigación

Lo que se pretende realizar, es el analizar los riesgos y construir por medio del firewall un sistema de control y seguridad único que ayude a proteger el sistema de la red de datos.

1.3.1 Límites teóricos

1.3.1.1 Diagnóstico del problema de investigación

La empresa cuenta con 14 máquinas conectadas en red hacia un rack central, además cuenta con un ISP que es TELCONET, decir también que la empresa cuenta con 2 servidores, una que es Servidor de Correo y la otra de FoxPro, cada uno de los servidores y computadores de la empresa, está expuesto a riesgos, la no adecuación o la implementación del firewall en la empresa, sigue corriendo riesgos, daños y posibles ataques de espías a la empresa, sabiendo que hoy en día en cada empresa media o pequeña, se debe manejar con un sistema único que ayuda a mejorar la seguridad corporativa o al menos que contrarreste posibles vulnerabilidades en los procesos de información.

Al no poseer un sistema seguro, los servidores propios de la empresa, se expone a diversos riesgos. Es por esta razón que la seguridad de la red global, depende de un sistema único.

1.3.1.2 Característica principal

Cada uno de los servidores y computadores de la empresa, está expuesto a riesgos, tales como espías, hackers, virus, daños de software y hardware, mala organización de flujo de datos en la red.

1.3.1.3 Característica(s) secundaria(s)

1. El no controlar la información de la red (Ips, nom_maquina, subred, etc.)

2. No existe Graficas que ayuden a entender el control organizativo en la red.

3. No existe registro o documentación de datos en la red.

4. No existe filtros o políticas de seguridad

1.3.2 Límites temporales

1.3.2.1 Tiempo que demora la investigación

El tiempo aproximado de la investigación de la tesis es de 4 meses. Tomando en cuenta que el tiempo que se emplea para su desarrollo y se establece de varias horas diarias

1.3.2.2 Series estadísticas acerca del problema de investigación

2009

El nivel de inseguridad a crecido de manera radical, sin saber el volumen de información que maneja la empresa, mediante finiquitar procesos de negociación, nacionales o internacionales mediante la web, de igual manera, han infectado de virus, daños en el quipo, también es importante indicar, el nivel de riesgos del manejo de la información.

2008

Antecedentes de constantes niveles de riesgo, por manejar procesos sumamente confidenciales y únicos para la empresa, basados en transferencias, cuentas de bancos, negocios nacionales o internacionales, entre otros.

1.3.3 Límites espaciales

Empresa: Frada Sport, dedicado a la confección de ropa deportiva, ubicado en la Cdla. Católica, (Serrano Abad y Miguel León, diagonal a la iglesia.)

1.4 Objetivos

1.4.1 Objetivo principal

Implementar un Sistema de control y seguridad Informático (firewall), que permita reducir riesgos y vulnerabilidades, estableciendo niveles de rendimiento y performance óptimos en el campus informático de la empresa Frada Sport.

1.4.2 Objetivos Específicos

- Determinar el tipo de debilidad de seguridad a nivel de la red, acorde a las necesidades y requerimientos de la Empresa.
- Crear un modelo de administración seguro, basado en el control y organización de datos en la red.
- Desarrollar un plan de control que permita al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados (SNORT)
- Establecer por medio del Firewall, un control y protección centralizada de un anti-spam y antivirus.
- Mejorar el rendimiento de los equipos y de la red, a través de políticas de seguridad para cada usuario de la empresa, permitiendo, denegando el acceso.
- Generar por medio del firewall, un análisis, para determinar el tráfico en la red entrante y saliente

1.5 Justificación de la investigación

1. ¿Para qué sirve el trabajo de graduación?

Para generar nuevas herramientas de tecnología que ayude a la empresa a utilizar proyectos que tenga gran relevancia técnica, así mismo, permitir aprender de herramientas actuales que facilita poder desenvolverse mejor el mundo actual de la tecnología acogiendo proyectos únicos de sistemas informáticos seguros.

2. ¿Cuál es la relevancia técnica?

La relevancia es de alto nivel, ya que el firewall posee una bitácora de software único de desarrollo.

3. ¿Ayudara a resolver algún problema práctico?

Ayuda a resolver los problemas que la empresa Frada Sport posee en la actualidad, que es la de no contar con herramientas de seguridad.

4. ¿El tema es de actualidad?

El tema es de mucha actualidad, y es novedoso que ayuda de mucho a las empresas a tener un control y seguridad de software y hardware.

1.6 Hipótesis

1.6.1 Hipótesis del trabajo de graduación

Hipótesis del trabajo de graduación
Si
Se propone medidas de control y seguridad (firewall)
Entonces
La empresa obtiene una mayor seguridad, en control de software, hardware, y reducir niveles de riesgo.

1.6.2 Variables del trabajo de graduación

1.6.2.1 Definición conceptual

Variable 1: Sistema de Seguridad Endian Firewall

Variable 2: Empresa Frada Sport (Confección de ropa deportiva)

Variable 3: Mecanismo de Control de organización en la red

1.6.2.2 Operacionalización de las variables

Variable	Dimensión	Indicador
Variable 1:	Sistema de Seguridad Endian Firewall	Software Funcional
Variable 2:	Empresa Frada Sport (Confección de ropa deportiva)	Empresa Frada Sport
Variable 1:	Mecanismo de Control de organización en la red	Software seguro y eficiente

1.7 Marco de referencia

1.7.1 Antecedentes teóricos del tema de investigación

Que autores de libros han escrito acerca del tema de investigación (cinco autores de libros con sus respectivos títulos, edición y año de edición

N|	Autor	Titulo	Editorial	año
1	Fco. Ferreyra Lopez	Firewall de alta disponibilidad		2009
2	DORA ANABELLA DIAZ VILLATORO	SISTEMAS DE CONTROL DE ACCESOS ENTRE REDES POR MEDIO DE'FIREWALLS		2010
3	Héctor Rodolfo Morales Rabanales	DISEÑO DE ASEGURAMIENTO DE REDES UTILIZANDO DMZ´S		2009
4	RECALDE ARAUJO, HENRY MARCELO;SALAS OCHOA, JUAN PABLO	APLICACION DE SOFTWARE QUE PERMITA DETECTAR Y NEUTRALIZAR INTRUSOS A NIVEL DE LA CAPA DE APLICACION, EN EL MODELO DE REFERENCIA TCP/IP		2008
5	Gómez, Marcelo	Diseño de una red wan para la empresa maderera Novopan del Ecuador S. A. y Codesa	QUITO / ESPE-H.CENEPA / 2007	2008

Tesis existentes en la universidad ecuatoriana

N|	Autor	Titulo	universidad	año
1	Ordóñez Galiano, Felipe Andrés	REDES DE DATOS FIREWALL SOFTWARE VYATTA VIRTUALIZACIÓN SEGURIDAD DE LOS DATOS	ESPE	2012
2	Cristian Guerra C	Implementación de una Red segura, utilizando dispositivos utm	POLITECNICA DEL EJERCITO	2011
3	MOYA CASTELLANO, FAUSTO SANTIAGO	SISTEMA EXPERTO DE ANALISIS DE SEGURIDAD Y SALUD EN EL TRABAJO DE LAS PYMES	UNIVERSIDAD TECNOLOGICA EQUINOCCIAL	2009

Cinco tesis relacionadas con su tema de tesis existentes en universidades extranjeras

N|	Autor	Titulo	Universidad extranjera	año
1	Diego Gagliardo	Los administradores Endian Firewall Guía		2009
2	Ferreyra Lopez	Firewall de alta disponibilidad	Vasco de Quiroga	2009
3	Roberto Sánchez Llamas	IMPLEMENTACION DE PROTOCOLO DE COMUNICACIONES MODBUS/TCP PARA LINUX EN LENGUAJE C++. APLICACIÓN SOBRE ANALIZADORES DE REDES SIEMENS SENTRON PAC4200	Universidad Politecnica de Cartagena	27 de julio de 2012
4	Ilich Hernán Liza Hernández	DISEÑO DE UNA RED LOCAL INALÁMBRICA UTILIZANDO UN SISTEMA DE SEGURIDAD BASADO EN LOS PROTOCOLOS WPA Y 802.1X PARA UN COMPLEJO HOTELERO	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	2009
5	Ampuero Chang, Carlos Enrique	Diseño de un sistema de gestión de seguridad de información para una compañía de seguros	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	2009

Cinco artículos de revistas indexadas existentes en la bases de datos del SENASCYT

N|	Autor	Titulo	Nombre Revista	año	Dirección electrónica
1	Ludeña González, Patricia	Estudio de aplicabilidad del estándar 802.11n para redes de larga distancia para entornos rurales en América Latina	TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES REDES DE LARGA DISTANCIA INTERNET ESTÁNDAR 802.11n IEEE ZONAS RURALES AMÉRICA LATINA	2011	
2	Blanco, Paula	Fase 2.3: Servicios de Internet y Seguridad	TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES INTERNET TELECOMUNICACIONES TRANSFERENCIA DE INFORMACIÓN INNOVACIONES TECNOLÓGICAS	2010	
3	Castro Guerrero, Carlos Alberto	Implementación de un Honeypot mediante KIPPO para detectar acciones de un atacante al ganas acceso por SSH para mejorar la seguridad en la red de un servidor	INFORMÁTICA CIBERNÉTICA HONEYPOT SEGURIDAD DE RED	2011	
4	Jonathan Ángeles García	GNU/LINUX Endian: Endian Firewall Security Appliance	GNU/LINUX Endian: Endian Firewall Security Appliance	2010	
5	Rocío Arango	Uso de Debian firewall casero	Uso de Debian firewall casero	2010	

1.7.2 Marco conceptual

N|	Concepto
1	Endian Firewall.- Sistema de seguridad único, open source.
2	Interfaces – Opciones de puesta en marcha. Modelos gráficos
3	Los gráficos de tráfico.-Puesta en marcha de los modelos de control
4	Conexiones.- Endian Firewall Modelos de control y comunicación
5	Estadísticas de correo SMTP.-Esta página le muestra gráficos de estadísticas sobre el proxy de correo SMTP.
6	DNS dinámico.- Conexión mediante dominios
7	RIESGO.- Nivel de inseguridad
8	Servidor.- Computadoras administradores
9	Filtro: Mecanismos Inteligentes
10	Antivirus: Impide ataques espías.
11	IDS: Sistema de Detección de Intrusos
12	Spamfilter configuración: Evita contenido malicioso, correo basura
13	Dominios.-Si ha habilitado el correo entrante y desea reenviar ese correo a un servidor de correo detrás del Endian Firewall
14	IPS: Sistema de Prevención de intrusos
15	Conexiones activas.- En esta página se puede ver todas las conexiones actualmente activas o inactivas
16	Dirección IP.-Proporcione la dirección IP que desea utilizar para la interfaz de la zona de una red.
17	Máscara de red.-Proporcionar la máscara de red que desea utilizar para la interfaz de la zona respectiva y la red detrás de él.
18	IP Estática.-Introduzca su dirección de IP pública de su proveedor le ha asignado. Si no tiene esta información, pregúntele a su proveedor.
19	Puerta.-La dirección IP de la puerta de entrada situada en el lado del ISP que se debe utilizar como puerta de enlace predeterminada.
20	DNCP: IP Automática

1.7.3 Marco jurídico

El marco jurídico, se acopla a la necesidad de involucrarse con niveles de riesgo, o dolosamente infiltrar o dañar medios de información, los cuales se involucra con sistemas información, ya sea software o hardware. Los niveles de seguridad con los que cuente una empresa, es de vital importancia para el desarrollo de medios de información seguros.

Es indispensable el correcto uso de técnicas y herramientas de seguridad, basado en manejar, manipular, controlar sistemas de información seguros.

En cualquier medio o entidad, se estructura normas, políticas, estrategias, para emprender estructuras a subordinados para alcanzar determinados resultados.

Si se violentara, o se dañara cualquier medio de información, la empresa ante sus normativas de políticas de seguridad, se involucran con los reglamentos ante las leyes de daños y perjuicios.

1.8 Metodología

1.8.1 Métodos generales que se va a utilizar en el trabajo de graduación

Inducción

El firewall, establece un control perimetral fiable y seguro, que comunica toda la red de datos, capaz de llevar a cabo un sistema que ayuda a la empresa, a poseer un nivel mayor de seguridad, basado en medios de control, vigilancia y estabilidad, además de incorporar sistemas inteligentes, capaz de receptar y examinar paquetes de datos seguros, mediante mecanismos centralizados.

Síntesis e Inductivo

La alta disponibilidad es un protocolo o sistema diseñado, que asegura un cierto grado absoluto de continuidad operacional de la empresa.

Las redes de datos tiene que ser configurado, en base en el sistema de seguridad, para producir la menor cantidad de tiempo de inactividad o falta de disponibilidad, la alta disponibilidad se puede conseguir mediante el buen uso de las herramientas que el hardware y software proporcionan para que la red sea única , por ejemplo, se pueden usar componentes redundantes.

Análisis

Se analiza e implementa, un sistema que ayuda a la empresa a tener un control organizativo de la red y mantener a software y hardware seguros.

Síntesis. Firewall de sistemas de control y seguridad.

1.8.2 Técnicas de Investigación que se van aplicar

1. Observación

Sin tener un control de organización y seguridad en la red, lo que provoca es la falta de organización a nivel de la red, es decir lo que se debe emplear, es crear políticas a nivel de usuario para dar paso o negar ciertas páginas de internet, tener un control de Ips, dominios, mascaras, etc. Para emplear una documentación organizativo en la red, también los servidores propios de la empresa, están expuestos a riegos tales como la infección de virus, ataques de espías, sin embargo, estos spam o virus los equipos de la empresa sean afectados en software y hardware, parar contrarrestar la inseguridad que hoy en día se está en auge.

2. Cuestionarios

En este punto, se aplican encuestas al personal y al gerente de la empresa Frada Sport para determinar los puntos críticos del de un sistema de control y seguridad.

3. Muestreo

Se aplican muestreos para determinar el grado de no control y seguridad de la empresa como tal.

Capítulo 2

Marco Teórico

TEORÍA APLICADA	DÓNDE FUE APLICADA	CÓMO SE APLICÓ	QUÉ RESOLVIÓ
Metodología de Investigación Científica Teoría para estructurar la metodología de investigación científica (Lazo, 2011)	Se aplica en todo el modelo de desarrollo del proyecto, metodología síntesis e inductivo.	Se aplica, en base al investigador, que reúne un conjunto de elementos que está provocando un problema determinado para llegar a establecer una solución y ejecutarla	Se resuelve, cumplir con la metodología en base a una serie de elementos dados, en una sola solución.
Fundamentos en Redes *Teoría para conocer fundamentos básicos en redes.* (Lykaios, 2011)	Se aplica como parte del conocimiento esencial para conocer el modelos de desarrollo	Se aplica todos los fundamentos utilizando elementos básicos, beneficios, conectividades, etc.	Es indispensable para fundamentar en base a los conocimientos teóricos para resolver modelos de desarrollo.
Modelo OSI *Teoría para conocer los niveles de capas en el modelo OSI.* (Ramírez, 2010)	Se aplica para conocer cada capa en función a los protocolos de comunicación	Se aplica conociendo y relacionando el nivel de capa con los protocolos de comunicación.	Se resuelve determinar que protocolo corresponde a cada capa del modelo OSI.

Modelo Tcp/Ip *Teoría para conocer las capas del modelo Tcp/Ip.* (Xperts, 2012)	Se aplica para conocer cada en función a los protocolos de comunicación	Se aplica conociendo y relacionando el nivel de capa con los protocolos de comunicación	Se resuelve determinar que protocolo corresponde a cada capa del modelo tcp/ip.
Protocolos Utilizados *Teoría para conocer los protocolos de comunicación* (Moguel, 2010)	Se aplica para conocer cada en función a los protocolos de comunicación	Se aplica relacionando el modelo OSI y tcp/ip contra los protocolos de comunicación	Se resuelve y se determina la funcionalidad de los protocolos en base a la aplicación EFW.
Protocolos y procesos de Comunicación en la Red *Teoría para conocer todos los protocolos, y procesos de comunicación en la red.* (Onofre, 2013)	Se aplica para conocer fundamentos de comunicación en la red	Se aplica en base a conocimientos teóricos para establecer niveles de conocimiento para emprender medios de seguridad.	Se resuelve determinar y conocer sus funcionalidades y procesos mediante los protocolos y elementos de la red.
Seguridad en Redes *Teoría para conocer niveles de seguridad en la red.* (CETINA, 2012)	Se aplica en toda la estructura física y lógica mediante el sistema de seguridad.	Se aplica en base a conocimientos esenciales sobre seguridad en redes.	Se resuelve determinar niveles de integridad, disponibilidad y confidencialidad mediante el sistema WFW.

Cálculo de la Muestra para Encuestas *Teoría para justificar técnicamente para cálculo de la muestra* (ASI, 2010)	Se aplica a los empleados de la empresa Frada Sport como parte de la población	Se aplica en base a una fórmula mundial aplicable a todo principio estadístico	Se resuelve justificar técnicamente para el cálculo de la muestra
Estadística Inferencial Teoría para cruzar la información en base a preguntas de la encuesta (Ponce, 2010)	Se aplica a los empleados de la empresa Frada Sport.	Se aplica, mediante el cruce de preguntas cerradas en base a los resultados de lo que espera la empresa.	Se resuelve y se genera, todas las problemáticas y el foco para emprender el desarrollo propuesto.
Análisis y Niveles de Riesgo *Teoría para conocer los niveles de riesgo de la empresa.* (Juan, Análisis y Niveles de Riesgo, Observacion Directa, 2013)	Se aplica a las áreas de la empresa Frada Sport.	Se aplica en base de un análisis fundamental para conocer niveles de inseguridad de la empresa.	Se resuelve establecer que áreas dentro de la empresa está expuesto a riesgos y posibles vulnerabilidades.
Diseño y Análisis de la Situación Actual de la Empresa Frada Sport *Teoría para conocer los niveles de riesgo en base a diseños de la situación actual.* (Juan, Diseño y Análisis de la Situación Actual de la Empresa, ObDirecta, 2013)	Se aplica a las áreas de la empresa Frada Sport.	Se aplica en base a diseños funcionales actuales de procesos de inseguridad.	Se resuelve y se apunta destacar que áreas dentro de la empresa está expuesto a posibles vulnerabilidades y peligros latentes.

Amenazas y Vulnerabilidades que presenta la empresa Frada Sport Teoría para estructurar mecanismos de peligro y procesos frágiles de datos de la empresa. (Ochoa, Julio 2012)	Se aplica en el proceso de manejo de información de la empresa.	Se aplica, conociendo todos los niveles de información que maneja la empresa, ya sea segura, o presentando posibles vulnerabilidades en su proceso de manejo.	Se resuelve, y se determina, qué áreas dentro de la empresa presenta niveles inseguros, y altamente confidenciales.
Metodología de Desarrollo T.A.M.A.R.A: Testeo, Análisis y Manejo de Redes y Accesos Metodología de desarrollo en base a procesos y etapas, en base a un sistema de control, seguridad y administración en la red. (María Fernanda Viteri Minaya, 2011)	Se aplica en todo el modelo de desarrollo del proyecto, basado en la metodología	Se aplica brindando protección, seguridad, y que refleja el objetivo de la metodología, en base a etapas y modelo de administración, seguridad, auto protección, entre otros.	Se resuelve en base a la metodología presentada, que sustenta el nivel de seguridad, en base a las necesidades de la empresa.

Sistema de Seguridad open source, abaratando costos, medidas de prevención basado en mecanismos de seguridad. En esta teoría, se basa en emprender e implementar el sistema de seguridad, reduciendo costos operativos. (Guerra, 2011)	Se aplica en el servidor propio de la empresa, basado en el Sistema Operativo CentOs.	Se mide características mínimas de hardware para empezar a instalar y configurar el sistema de seguridad, basado en las necesidades de la empresa.	Se resuelve, tener un sistema único de seguridad y sobre todo, en un sistema abierto, para futuras herramientas de administración en base a las necesidades de la empresa.
Modelo de administración mediante, control y organización de los datos en la red, basados en subprocesos (sistema, estado, red y registros del endian firewall) de toda la información que pasa a través de la red. En esta teoría, se basa en conocer métodos de seguridad y control que administración del sistema de seguridad. (Macías, 2011)	Se aplica en la red global de datos, de la empresa Frada Sport.	Se aplica en base a modelos de control y organización de datos en la red, en el cual su administración y rendimiento efectúa su alta disponibilidad.	Se resuelve, contar con subprocesos de control y vigilancia de la red global de datos para su correcta administración

Endian firewall Intrusion Prevention En esta teoría, es parte del sistema de seguridad Efw, que regula los sistemas de prevención de intrusos. (Alfaro, 2011)	Se aplica en la red global de datos, de la empresa Frada Sport	Se aplica, conociendo la arquitectura, las reglas, y el conjunto de paquetes snort, para saber su funcionamiento IPS.	Se resuelve, en base al acceso a la web o programas que son medios altamente riesgosos por su contenido malicioso.
Control y protección de los datos por medio de un antivirus y anti-spam (métodos inteligentes) Centralizados En esta teoría, es denominado, métodos inteligentes de alta disponibilidad centralizados. (Shram, 2010)	Se aplica en la red global de datos, de la empresa Frada Sport	Se aplica, en base a toda la red de datos, los denominados motor de antivirus (clamav) y entrenamiento antispam centralizados.	Se resuelve, en base a los usuarios de acceso a la web, permitir seguridad al ingreso de dichas páginas, así no se sepa identificar riesgos.

Mejorar el rendimiento de los equipos, (servidor proxy, autenticación, contenido de filtros, políticas de acceso) En esta teoría, maneja mecanismos únicos para poder segmentar la red de datos, en base a los empleados de la empresa. (Elit, 2011)	Se aplica en la red global de datos, de la empresa Frada Sport	Se jerarquiza o se segmenta la red, de acuerdo a los niveles de los empleados, para crear medios o políticas de seguridad altamente disponibles	Se resuelve, crear políticas de seguridad, como medio de la correcta administración, control avanzado, basado en mejorar el rendimiento de los equipos informáticos.
Tráfico entrada y salida de datos En esta teoría, abarca regular y vigilar todo el tráfico entrante y saliente de la red de datos (Merino, 2011)	Se aplica en la red global de datos, de la empresa Frada Sport	Se establece analizar la fluidez de los datos, en los días de labores y los fines de semana para administrar el tráfico entrante y saliente.	Se resuelve, administrar, vigilar, controlar, la red global de datos, en estadísticas gráficas que proporciona el EFW, en base a políticas de seguridad posteriores.

CAPÍTULO 3

3.1 METODOLOGÍA DE LA INVESTIGACIÓN [1]

3.1.1 Unidad de Análisis

Para establecer y garantizar el estudio y análisis del proyecto, es de suma importancia, mantener vínculos con la empresa para conocer todos los niveles del manejo de cada proceso, misma que se es necesario para mantener y brindar seguridad total contra posibles amenazas y vulnerabilidades.

3.1.2 Tipo de Investigación

El tipo de investigación que se aplica, es la de metodología aplicada en base a documental.

Documental.- Se identifica y se establece la búsqueda de información, correspondiente a una forma de contenidos, libros, revistas, artículos y manuales, que es necesario para poder emprender y formar parte de la seguridad física y lógica del rendimiento de los equipos.

3.2 Metodología de Investigación Científica

Es necesario la utilización de la metodología, en este caso, se aplica el método de ***síntesis***, ya que consiste que el investigador, reúna un conjunto de elementos que está provocando un problema determinado para llegar a establecer una solución y ejecutarla, también reúne una serie de proceso y mecanismos a seguir en un orden determinado, para generar un grado de solución adecuado y en secuencia para cada proceso, también el método ***inductivo*** que generaliza todas actividades de la administración de seguridad y el área en que se desenvuelven.

3.2.1 Técnicas

Se utiliza las técnicas de la investigación, basado en las encuestas, y muestreo para la obtención de todo un conjunto y recolección necesaria para cada caso.

3.2.2 Instrumentos

Se utilizara instrumentos metodológicos y tecnológicos tales como: Encuestas descriptivas y Análisis e interpretación cruzada, también Internet.

---

[1] Metodología de la Investigación

3.3 Fundamentos Teóricos:

3.3.1 Fundamentos en Redes. [2]

3.3.2 Introducción a las Redes de Datos

Las redes de datos, es un sistema que determina el enlace de varios puntos o terminales, basado en un medio físico, en el cual, su objetivo destaca el envío y recepción de determinados paquetes de información. Además representa una estructura básica de integración, basada en:

- Armario de telecomunicaciones, donde se interconecta con hubs, pach panels.
- Servidores propios que se encuentran disponibles. (Sistemas base)
- Hubs, amplifican señales, se encuentra conectada entre nodos, la cual utiliza cable utp, fibra óptica, entre otros.
- Patch Panel.- se basan en organizar los puntos de control
- Patch core.- son cables de comunicación, las cuales están inter conectadas con los puntos de acceso o terminales pcs, en donde los **elementos principales de una red** es: Servidores, cliente, medio, datos compartidos, recursos.

3.3.3 Beneficios de las Redes de Datos.

Teniendo presente la disponibilidad de los medios informáticos, la red de datos comunica a todas las personas, empresas y el mundo, la red de datos, ejemplifica la eficiencia de la comunicación y los costos mínimos, además compone procesos basados en el compartir información, hardware y software, y medios de administración con soporte centralizado, en donde **se centra en una red basada en "servidor"**, a lo que es llamado para brindar servicios con rapidez a petición de un cliente de la red garantizando la seguridad.

3.3.4 Conectividad

Lan: (Local Área Network) Ejemplifica la red de area local, especifica la conexión de ordenadores y periféricos en una empresa pequeña o mediana.

Man: (Metropolitan Área Network) Red metropolitana, para empresas grandes, es de alta velocidad, maneja una cobertura extensa geográfica, estructura la transmisión de información de múltiples servicios.

Wan: (Wide Área Network) Es una red de área amplia, esta conectividad, cumple distancias de 100 a 1000 Km, brinda servicios medianos y amplios.

[2] Recuperado: Fundamento en Redes: http://tareastecisc.blogspot.com/2011/03/unidad-1-fundamentos-teoricos-de-redes.html

3.4 Modelo OSI [3]

El modelo Osi, representa las capas de los protocolos de comunicación, cada una de los diferentes niveles, representa funciones definidas, cabe mencionar, que el modelo como tal, no representa una arquitectura, sino las acciones que cumple cada capa, es de vital importancia, enfocarse al modelo Osi, para conocer su funcionalidad.

Niveles o Capas

Imagen n°1: Modelo Osi

- ✓ Capa Física.- Esta dirigida a a la transmisión de bits, en forma seguida a lo largo del canal comunicación, principalmente, destaca que si llega un dato con valor 0 o 1, llega al otro lado de igual manera.

- ✓ Capa de Enlace.- Principalmente, dirigida a la corrección de errores, esta capa transmite grupos de paquete de datos, denominados tramas.

- ✓ Capa de Red,. Dirigida a al control de la subred, se centra en el conocimiento de la topología de la red, y decide la ruta que va a ser enviada la información evitando el congestionamiento.

[3]Recuperado Modelo OSI: http://www.institutomardecortes.edu.mx/apuntes/quinto/hprod2/unidadIII.pdf

- ✓ Capa de Transporte.- Principalmente encardada de fragmentar de manera correcta el recibimiento de los datos para ser enviada a la cada de red, de forma que se asegura la llegada y el correcto grupo de paquetes de datos a su destino.

- ✓ Cada de Sesión.- Capa accesible al usuario y multiusuario, encargada de la comunicación de los hosts.

- ✓ Capa de Presentación.- Apunta a preservar el significado de la información recibida, su objetivo es codificar los datos de la transmisión del flujo de bits, adecuada para la transmisión y después codificarlo para ser presentada en el formato del destino.

- ✓ Cada de Aplicación.- Involucra programas del usuario, además contiene protocolos de utilización frecuentemente.

  Cabe mencionar el manejo de protocolos genéricos, no a los protocolos de capa de aplicación Osi, se destaca:

  - ❖ HTTP
  - ❖ FTP
  - ❖ SMTP
  - ❖ POP
  - ❖ SSH
  - ❖ TELNET

3.4.1 Modelo Tcp/Ip [4]

Este modelo se enfoca a una serie de protocolos enfocada al internet, y que permite la transmisión de datos entre las redes de computadoras.

Este modelo, hace referencia a dos protocolos importantes que son, protocolo de control de transmisión y protocolo de internet, son los más utilizados, además el modelo tcp/ip, en la fuente de acceso a internet, destaca el enlace con computadoras de diferente sistema operativo.

Capa físico.- Se orienta a las características físicas de la comunicación, y los detalles con la conectividad, códigos,, canales modulación, señales, distancias, etc.

Capa Enlace de Datos.- Destaca, el cómo viaja el paquete de datos sobre el nivel físico, así como campos de cabecera de trama que especifica las maquinas a ser destinadas en el conjunto de datos, es decir Ethernet, wireless, Token Ring , etc.

[4] Recuperado Modelo Tcp/Ip: http://mikrotikxperts.com/index.php/configuraciones/conocimientos-basicos/159-modelo-osi-y-tcp-ip

Capa Internet.- Esta capa, soluciona de transporte orientada a la fiabilidad y sobre todo la seguridad de los datos en que llegue a su correcto orden, también determina a que aplicación o medio que va llegar los paquetes de datos.

Capa de Aplicación.- Se orienta a los programas comunes para la comunicación con la red de datos con otros programas, apunta a las especificaciones que procesa los datos a nivel de aplicación en el formato que se use para ser codificado, se trabaja con aplicaciones de usuario, además manejan protocolos http ftp smtp, dns,etc.

3.5 Protocolos Utilizados[5]

Protocolos	Dónde se aplica
HTTP	Servidor Proxy (configuración proxy, políticas de acceso, autenticación, filtros, antivirus)
IP	Usuarios en la red.
UDP	Segmentación red
SMTP	Servidor Proxy, antivirus, coreo no deseado
FTP	Subida y transferencia de archivos, segmentación red
POP3	Filtros de correo no deseado
ICMP	Sistema de Seguridad Snort

3.5.1 Protocolos Utilizados en relación al sistema Endian Firewall

Capa de Aplicación	**HTTP, FTP**
Capa de Transporte	**TCP,UDP**
Capa de Red	**IP, ICMP**
Capa de Enlace	**Ethernet**

3.5.2 Definición de Protocolos y procesos de Comunicación en la Red (Protocolo Osi Capa 7)[6]

LAN.- Red de Área local, la LAN, interconecta varios dispositivos de red apuntando a una red de distancia corta, su comunicación, trasciende cableado de comunicación coaxial, par trenzado, fibra óptica.

[5] Protocolos Utilizados
[6] Protocolos de Comunicación en la Red, Osi capa 7

IP.- Protocolo de Internet, es una etiqueta numérica que se establece de una manera lógica y ordenada interfaces de comunicación de dispositivos de red, principalmente en una red de datos, se utiliza protocolos de internet que corresponde al nivel de red del protocolo TCP/IP.

TCP.- Protocolo de control de Transmisión, establece y forma el núcleo del funcionamiento conjuntamente con la Ip, se estructura a la capa 4 del Modelo Osi, apunta a mantener confiabilidad, en la comunicación de datos.

UDP.- Protocolo de Nivel de transporte, principalmente intercambia datagramas, establece la comunicación de enviar datagramas, su envió de datos, no confirma que los datos lleguen de manera fiable, correcta a los demás protocolos de comunicación.

SMTP.- Protocolo Simple de Transferencia de Correo, pertenece a la capa de aplicación, este protocolo, se basa en el texto de utilización para intercambiar mensajes de correo electrónico entre pc, dispositivos en una red de datos.

DNS.- Sistema de nombre de dominio, ejemplifica la traducción de dominio, ejemplo, www.fradasport.com.ec a un direccionamiento Ip.

FTP.- Protocolo de transferencia de archivos, además es un protocolo de transferencia de archivos, interconectados a la red tcp, para establecerse en una arquitectura cliente – servidor.

POP3.- Cuentas de email de correo electrónico, mensajes que se eliminan del servidor, es decir, los mensajes no se encuentran disponibles en un servidor correo web.

ICMP.-Es un protocolo de de mensajes de control de internet, protocolo de control y notificaciones de errores, apuntando por ejemplo, que un servicio no esté disponible.

3.6 Seguridad en Redes[7]

En la actualidad, se manejan diferentes avances en la tecnología, de igual manera, las amenazas y vulnerabilidades se ven atacado a las redes públicas o privadas, al punto de no existir redes seguridad, ópticas sino únicamente redes fiables, entiéndase red fiable, a la que apunta o se orienta a responder tal y como el planeador de la misma espera que realice, es decir, está enfocada a la creación de políticas de seguridad, al punto de no se fácilmente vulnerable.

Entonces es de vital importancia, poseer una red fiable enfocada a ciertos aspectos importantes, basados en:

- Integridad.
- Disponibilidad
- Confidencialidad

Confiable, basado en la red de datos, permita establecer accesos a personas autorizadas, es decir, no difundir privilegios con entidades externas a sistemas o procesos del sistema.

Disponible, enfocado a los elementos a la red, a brindar acceso mediante segmentaciones en la red de usuarios únicos de privilegios.

Integridad.- Dirigidos a los elementos de la red de datos, que podrán modificar accesos, privilegios, quienes estén autorizado sa hacerlo, todos los grupos de usuarios forman un todo, una red global de datos segmentados para formar un conjunto organizado y robusto en cuanto a seguridad.

El proceso de investigación, enfocado a la seguridad de la red, apunta a generar e integrar un solo medio o dispositivo en la red global de datos, basados en los elementos de integración logia, dirigidos, al control centralizado IPS, Clamav Antivirus, Trafico en la red, Segmentación en la Red, entre otros.

De tal manera, que la red, sea operativa con el propósito de fomentar las características sustentadas basadas en la integración disponibilidad, confidencialidad.

[7] Seguridad en Redes

Características de un sistema seguro:

- **Integridad**.- Se determina si se alterado los datos, garantizando que los datos sean lo que se supone que es.
- **Confidencialidad.**- Información legible para determinados usuarios
- **Disponibilidad**.-Siempre se encuentre disponible
- **No repudiación**.- Su uso, alteración de un usuario, el cual no debe negar su acción.

3.6.1 Squid

Destaca su amplia variedad de usos múltiples, empezando a destacar el servidor proxy y cache, también el buscar grupo de procesos que comparten medios de recursos en la red para obtener una mayor seguridad del tráfico, principalmente usado en los protocolos de comunicación HTTP, FTP, entre otros.

Funciona como un programa de servidor intermedio y contenido de red para comunicarse con los protocolos, es un servidor intermedio de alto rendimiento, lo que hace posible que sea confiable, seguro, el cual equipa un código libre.

3.6.2 Servidor Proxy

Un servidor proxy, establece comunicación intermedia entre un explorador web, por ejemplo (internet explorer, mozilla firefox, entre otros) e internet, estos actúan de manera que ayudan a mejorar el rendimiento en la web, presto que almacena copias de paginas más utilizadas, El servidor proxy, es muy utilizada en medianas y grandes empresas, muy diferente a comunicarse en una casa que no es aplicable.

Funcionamiento

Describe principalmente cuando un explorador solicita una página de internet almacenada en su cache del servidor proxy, lo cual mencionado servidor proxy lo administra, lo que resulta de una manera más sencilla y rápida consultar la web.

Principalmente el servidor web, apunta a mejorar y administrar la seguridad en el cual previene la filtración de contenido web altamente malicioso.

Además funcionan como cortafuegos y filtro de contenidos con mecanismos de seguridad Isp, para filtrar solicitudes de contenido para ciertas páginas de internet.

3.7 UTILIZACION DE IP FIJA CONTRA WIFI O REDES INALÁMBRICAS

Se tiene en cuenta que en la actualidad se maneja procesos únicos y más fáciles, es por esta razón que en cualquier empresa, el medio de conectividad que se utilice depende de las políticas o reglas que maneje dicha entidad.

Por ejemplo es fácil conectarse a una red pública o privada, de una manera sencilla, lógica, centralizada como es la conectividad wi fi, ya sea en una computadora portátil, tablet, entre otros.

Pero también se tiene en cuenta los modos de inseguridad que ahí se presenta, con un tipo de software determinado, se puede romper las reglas de seguridad, claves de acceso a información no autorizada, acceso a base de datos, acceso a información de datos de una empresa, e incluso dañar dolosamente los medios de información e informáticos, sabiendo que hoy en día los centros de administración de cualquier entidad, se encuentran expuestos a diferentes riegos y posibles vulnerabilidades en puntos críticos dados.

Es por esta razón que la utilización de estructuras o manejos de ip fija maneja un proceso mejor, seguro, lógico y determinante para establecer una correcta administración de procesos seguros y controlados, a pesar que no se maneje modos más fáciles de conectividad y modernos con simple conectividad.

3.8 Cálculo de la Muestra para Encuestas[8]

Para estudiar la empresa, se aplica la encuesta, basada principalmente en obtener informacion dada en la situacion actual y problematica central de diferentes procesos, para el cual se utiliza el cálculo de la muestra basada en la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

$$n = \frac{1{,}96^2 \text{ X } 0{,}5 \text{ X } 0{,}5 \text{ X} 12}{(12\text{-}1) \text{ X } 0{,}05^2 + (1{,}96^2 \text{ X } 0{,}5 \text{ X } 0{,}5)}$$

$$n = \frac{11.5248}{0.9879}$$

$n = 11.6$

N=Numero de elementos de la muestra (12)
e= Margen de error o imprecisión permitido (0.05)
Z= Valor critico correspondiente al nivel de la confianza elegido (95%, 1.96)
P= Proporción de la población (0.5)
Q= (1-P) (0.5)

Justificativo técnicamente para cálculo de la muestra:

La muestra a considerar es de *11* personas al trabajar con una población de 12 empleados que laboran en la empresa Frada Sport, lo cual cumple técnicamente el cálculo de la muestra justificada.

[8] Cálculo de la muestra para encuestas

3.9 Descripción – Análisis e Interpretación

ENCUESTA

PREGUNTAS OPCIÓN MULTIPLE

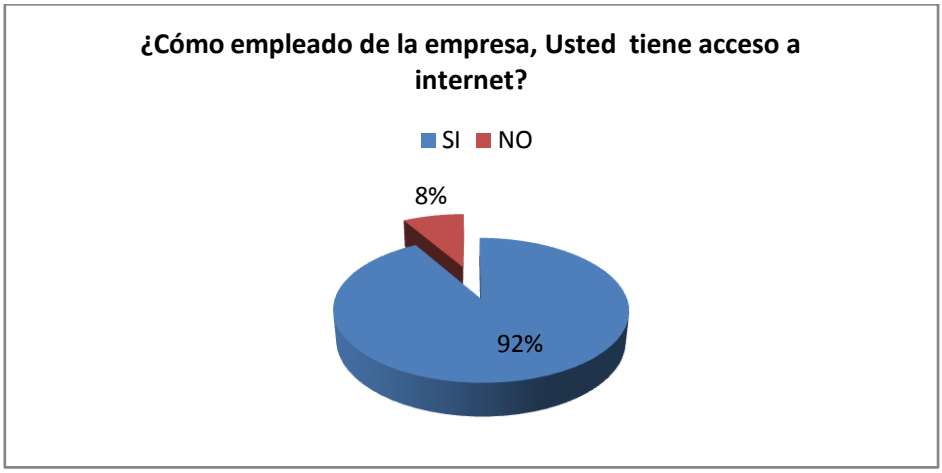
Encuesta realizada a los empleados de la empresa Frada Sport

- Muestra tomada a 12 personas que trabajan en el área Administrativa de la Empresa Frada Sport

- **¿Cómo empleado de la empresa, Usted tiene acceso a internet?**

Si ☐ No ☐

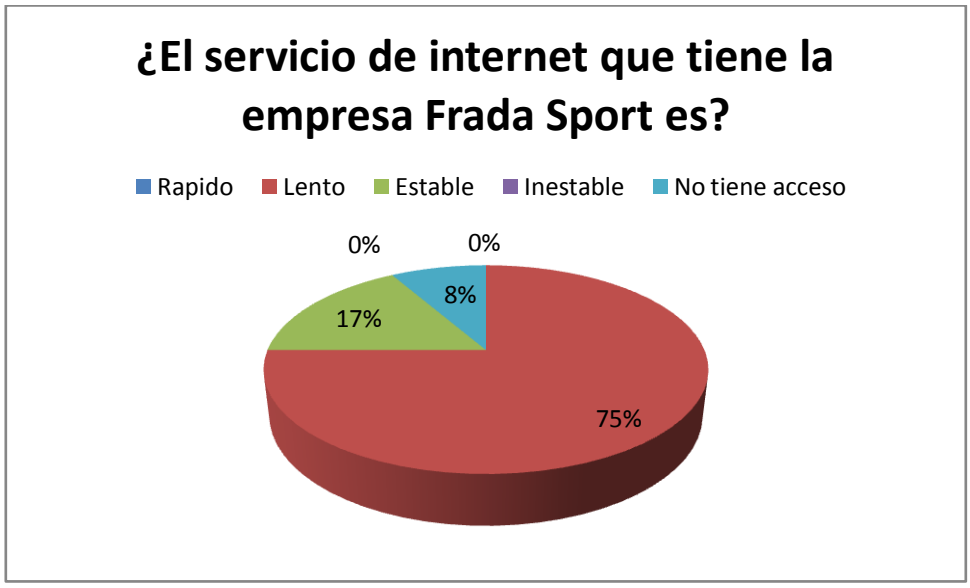
RESULTADO	DATOS	PORCENTAJE
SI	11	92%
NO	1	8%
TOTAL	12	100%



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 92% de la muestra, Si tienen acceso a internet, y un 8%, No tiene acceso a internet.

- **¿El servicio de internet que tiene la empresa Frada Sport es?**
  1. Rápido
  2. Lento
  3. Estable
  4. Inestable
  5. No tiene acceso

RESULTADO	DATOS	PORCENTAJE
Rápido	0	0%
Lento	9	75%
Estable	2	17%
Inestable	0	0
No tiene acceso	1	8
TOTAL	12	100%

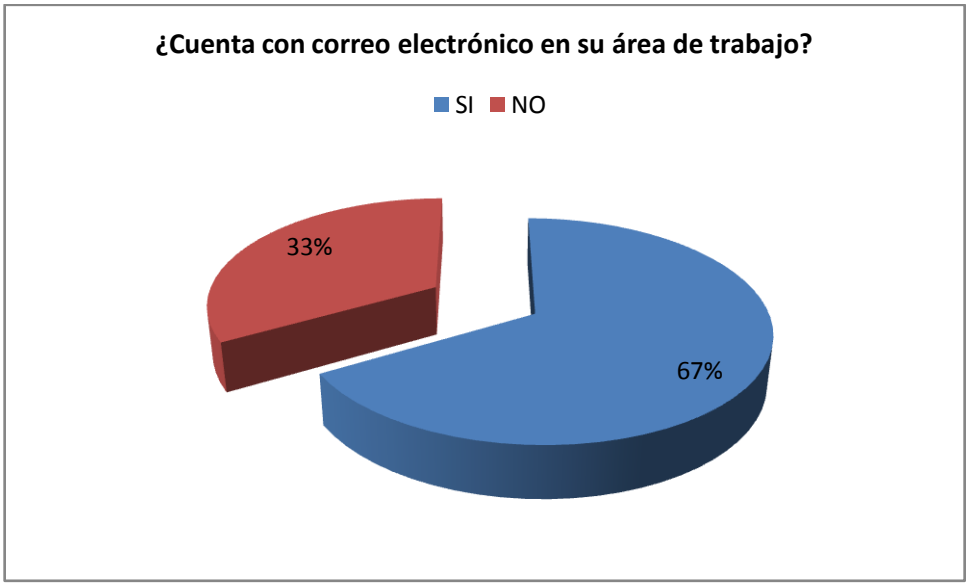


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 75%, indican que el servicio de internet que tiene la empresa es lento, y un 17%, indican que es estable.

- **¿Cuenta con correo electrónico en su área de trabajo?**

Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	8	33%
NO	4	67%
TOTAL	12	100%

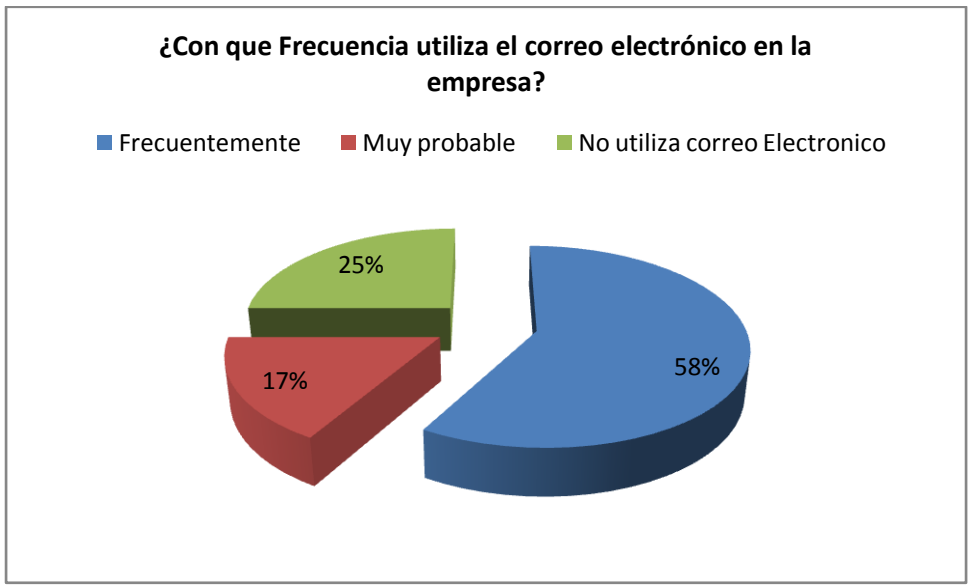


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 67%, Si poseen correo electrónico en su área de trabajo, y un 33%, indican que No poseen correo electrónico.

- **¿Con que Frecuencia utiliza el correo electrónico en la empresa?**

1. Frecuentemente
2. Muy probable
3. No utiliza correo electrónico

RESULTADO	DATOS	PORCENTAJE
Frecuentemente	7	58%
Muy probable	2	17%
No utiliza correo Electrónico	3	25%
TOTAL	12	100%

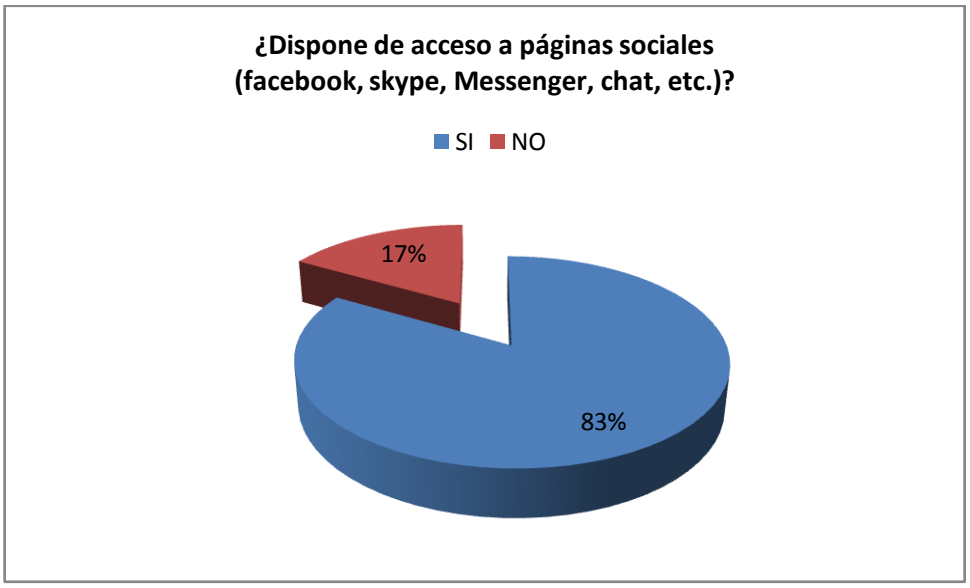


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 58%, frecuentemente utilizan el correo electrónico en la empresa, un 25%, indican que frecuentemente, no utilizan correo, y un 17%, mencionan que la muy probable utilizan frecuentemente el correo electrónico.

- **¿Dispone de acceso a páginas sociales (facebook, skype, Messenger, chat, etc.)?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	10	83%
NO	2	17%
TOTAL	12	100%

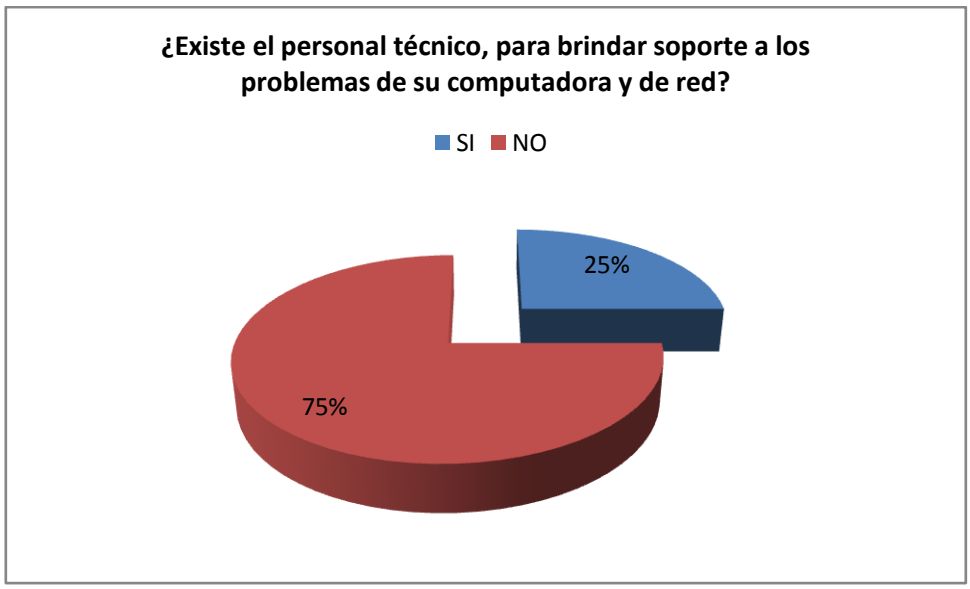


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 83%, Si disponen de acceso a páginas sociales (facebook, skype, Messenger, chat, y un 17%, indican que No poseen acceso a páginas sociales.

- **¿Existe el personal técnico, para brindar soporte a los problemas de su computadora y de red?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	3	25%
NO	9	75%
TOTAL	12	100%

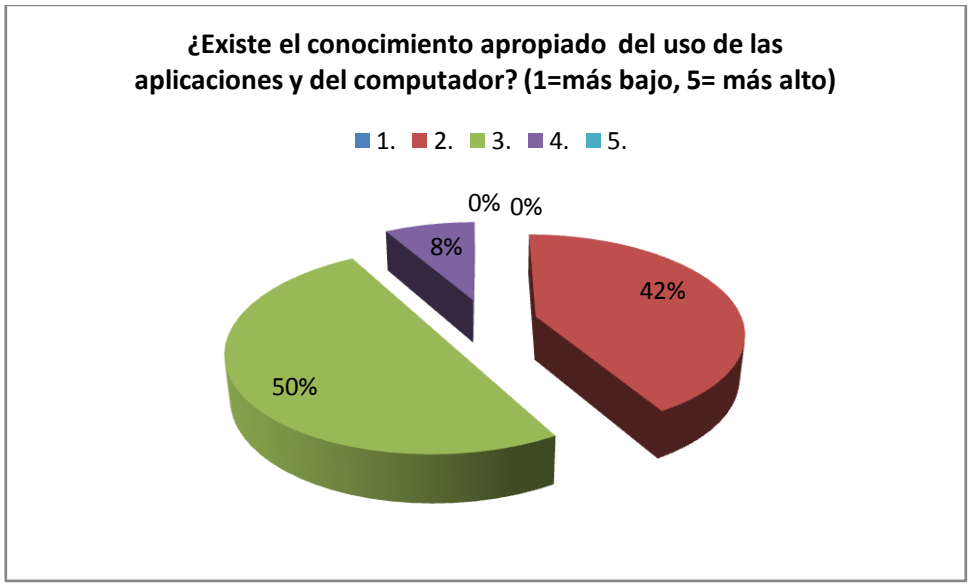


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 75%, No existe el personal técnico, para brindar soporte a los problemas de su computadora y de red, y un 25%, indican que Si poseen personal técnico.

- **¿Existe el conocimiento apropiado del uso de las aplicaciones y del computador? (1=más bajo, 5= más alto)**

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

RESULTADO	DATOS	PORCENTAJE
1.	0	0%
2.	5	42%
3.	6	50%
4.	1	8%
5.	0	0%
TOTAL	12	100%

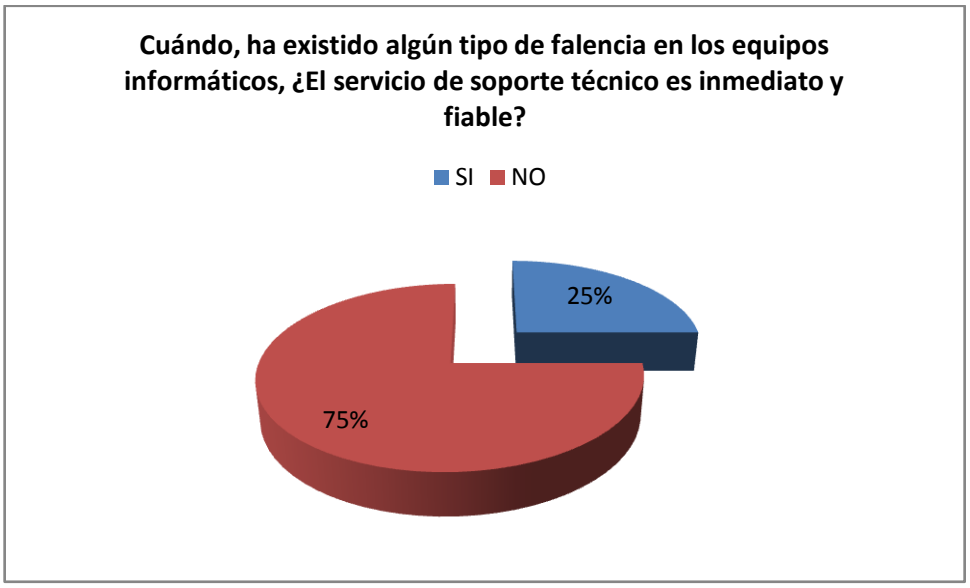


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 50% y 8%, tiene el conocimiento apropiado del uso de las aplicaciones y del computador, y un 42%, indican que no tienen el conocimiento apropiado.

- **Cuándo, ha existido algún tipo de falencia en los equipos informáticos, ¿El servicio de soporte técnico es inmediato y fiable?**

Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	3	25%
NO	9	75%
TOTAL	12	100%

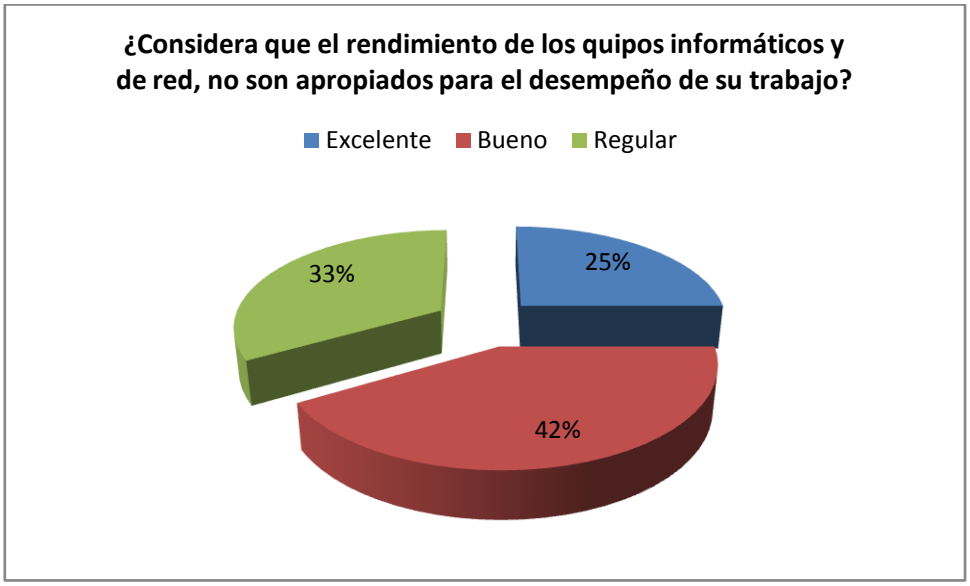


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 75%, cuando se ha presentado falencias en los equipos informáticos, El servicio de soporte técnico, No ha sido inmediato y fiable, y un 25%, indican que, cuando se ha presentado falencias en los equipos informáticos, El servicio de soporte técnico, Si ha sido inmediato y fiable.

- **¿Considera que el rendimiento de los quipos informáticos y de red, no son apropiados para el desempeño de su trabajo?**

    1. Excelente
    2. Bueno
    3. Regular

RESULTADO	DATOS	PORCENTAJE
Excelente	3	25%
Bueno	5	42%
Regular	4	33%
TOTAL	12	100%

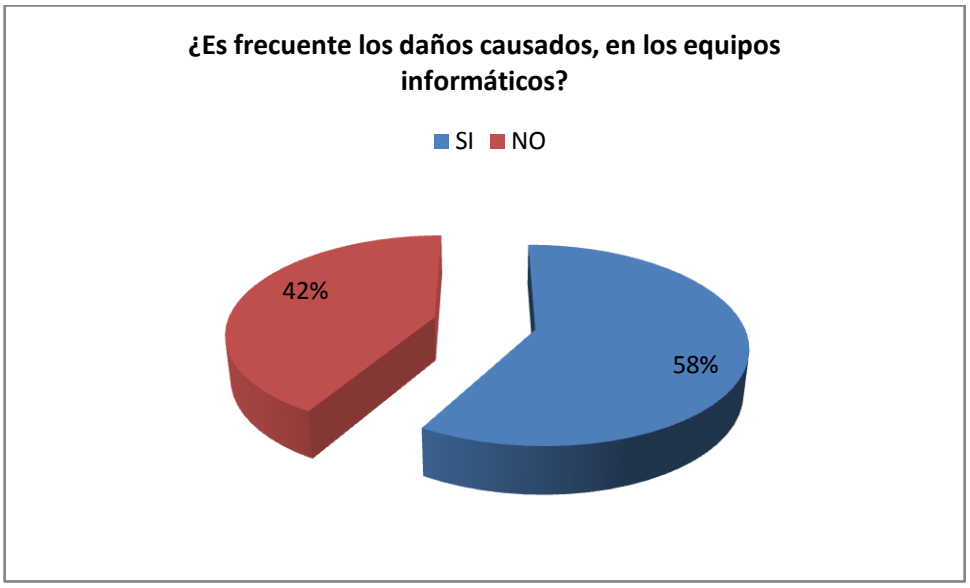


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 42%, Considera que el rendimiento de los quipos informáticos y de red, no son apropiados para el desempeño de su trabajo**,** un 33%, Consideran que el rendimiento de los quipos informáticos y de red, no son apropiados para el desempeño de su trabajo**,** un 25%, indican que Consideran que el rendimiento de los quipos informáticos y de red, no son apropiados para el desempeño de su trabajo.

- **¿Es frecuente los daños causados, en los equipos informáticos?**

Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	7	58%
NO	5	42%
TOTAL	12	100%

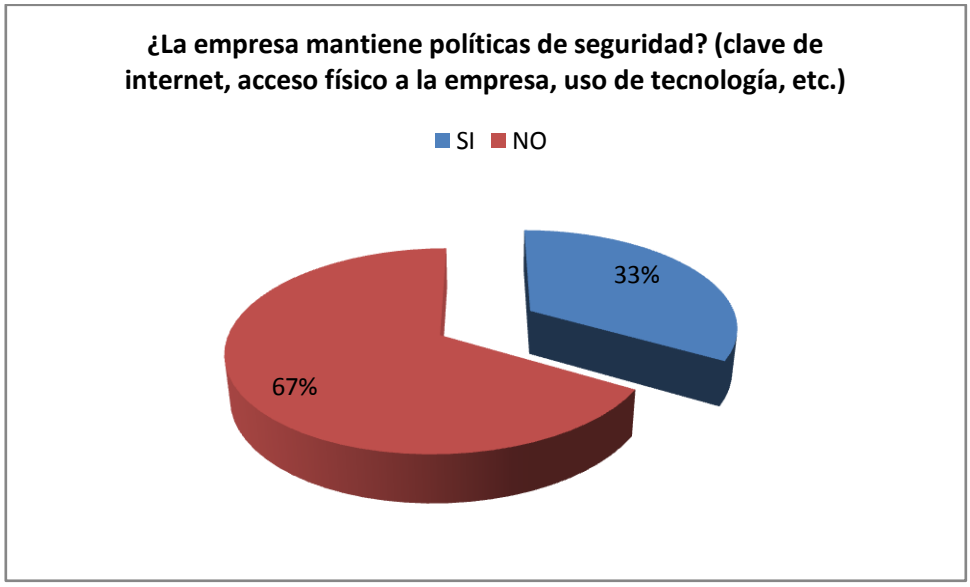


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 58%, considera que Si es frecuente los daños en los equipos informáticos, un 42%, indican que No es frecuente, los daños en los equipos informáticos.

- **¿La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	4	33%
NO	8	67%
TOTAL	12	100%

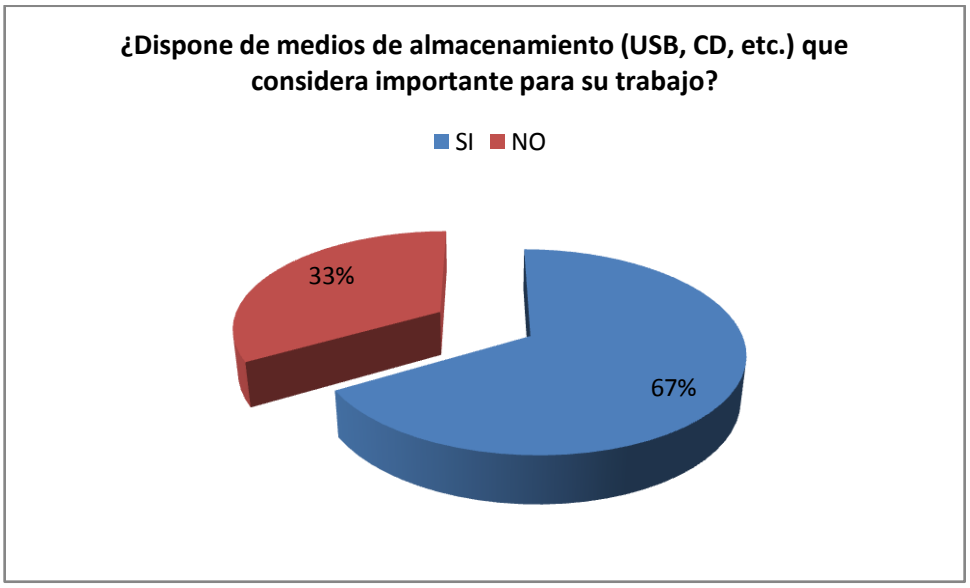


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 67%, No mantiene políticas de seguridad, y un 33%, indican que si poseen políticas de seguridad.

- **¿Dispone de medios de almacenamiento (USB, CD, etc.) que considera importante para su trabajo?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	8	67%
NO	4	33%
TOTAL	12	100%

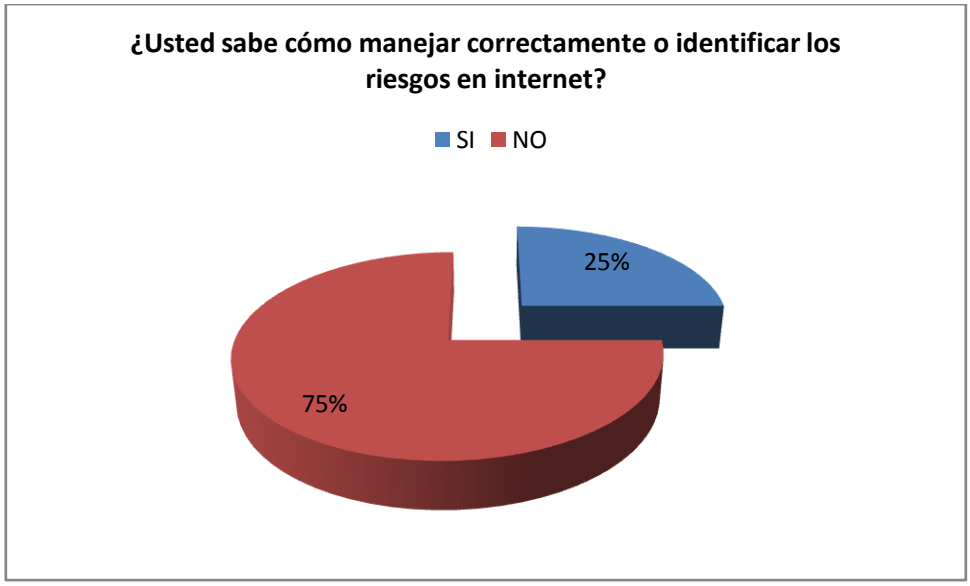


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 67%, Si dispone de medios de almacenamiento (USB, CD, etc.) que considera importante para su trabajo, y un 33%, indican que no dispone de medios de almacenamiento (USB, CD, etc.) que considera importante para su trabajo.

- **¿Usted sabe cómo manejar correctamente o identificar los riesgos en internet?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	3	25%
NO	9	75%
TOTAL	12	100%

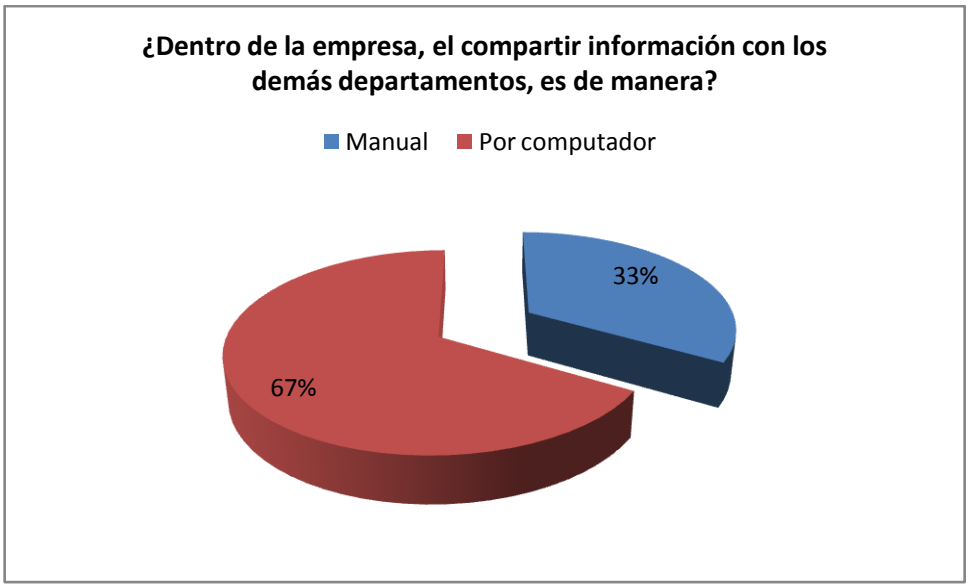


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 75%, No saben cómo manejar correctamente o identificar los riesgos en internet, y un 25%, indican que Si saben cómo manejar correctamente o identificar los riesgos en internet.

- **¿Dentro de la empresa, el compartir información con los demás departamentos, es de manera?**

  Manual ☐ Por Computador ☐

RESULTADO	DATOS	PORCENTAJE
Manual	4	33%
Por computador	8	67%
TOTAL	12	100%

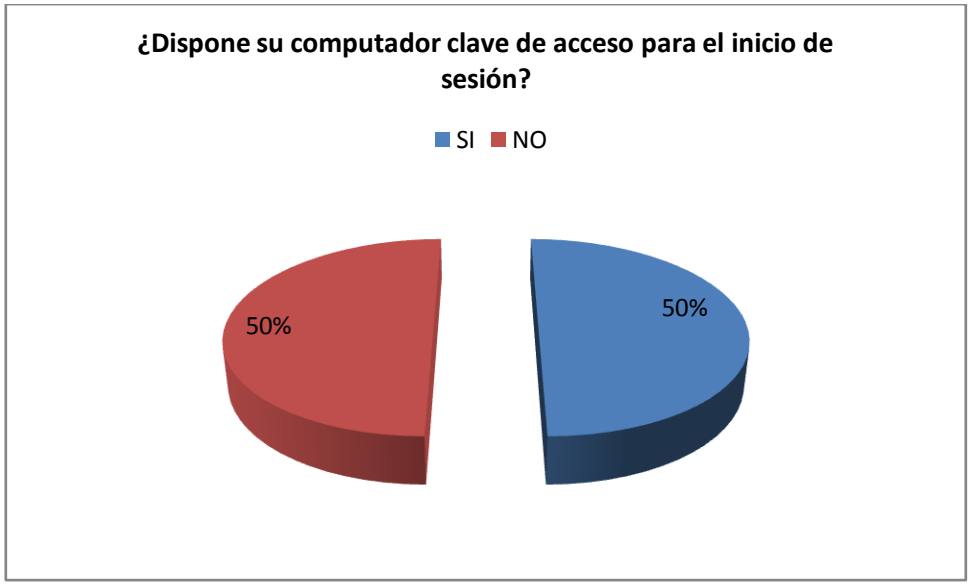


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 67%, el compartir información con los demás departamentos, es de manera por el Computador, y un 33%, indican que el compartir información con los demás departamentos, es de manera Manual

- **¿Dispone su computador clave de acceso para el inicio de sesión?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	6	50%
NO	6	50%
TOTAL	12	100%

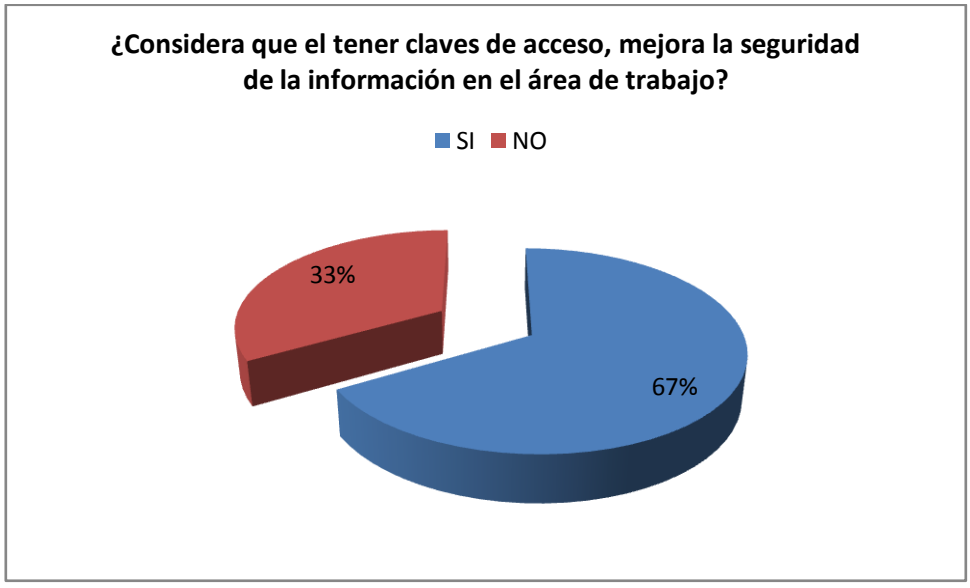


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 50%, Si Dispone su computador clave de acceso para el inicio de sesión, y un 50%, indica que No Dispone su computador clave de acceso para el inicio de sesión.

- **¿Considera que el tener claves de acceso, mejora la seguridad de la información en el área de trabajo?**

  Si ☐ No ☐

RESULTADO	DATOS	PORCENTAJE
SI	8	67%
NO	4	33%
TOTAL	12	100%

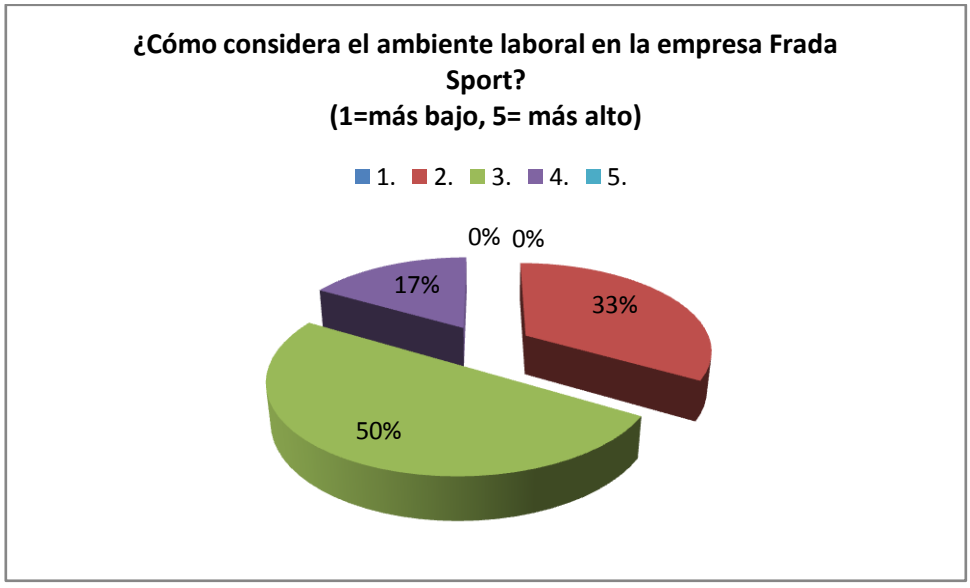


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 67%, Si Considera que el tener claves de acceso, mejora la seguridad de la información en el área de trabajo, y un 33%, No Considera que el tener claves de acceso, mejora la seguridad de la información en el área de trabajo

- **¿Cómo considera el ambiente laboral en la empresa Frada Sport? (1=más bajo, 5= más alto).**

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

RESULTADO	DATOS	PORCENTAJE
1.	0	0%
2.	4	33%
3.	6	50%
4.	2	17%
5.	0	0%
TOTAL	12	100%

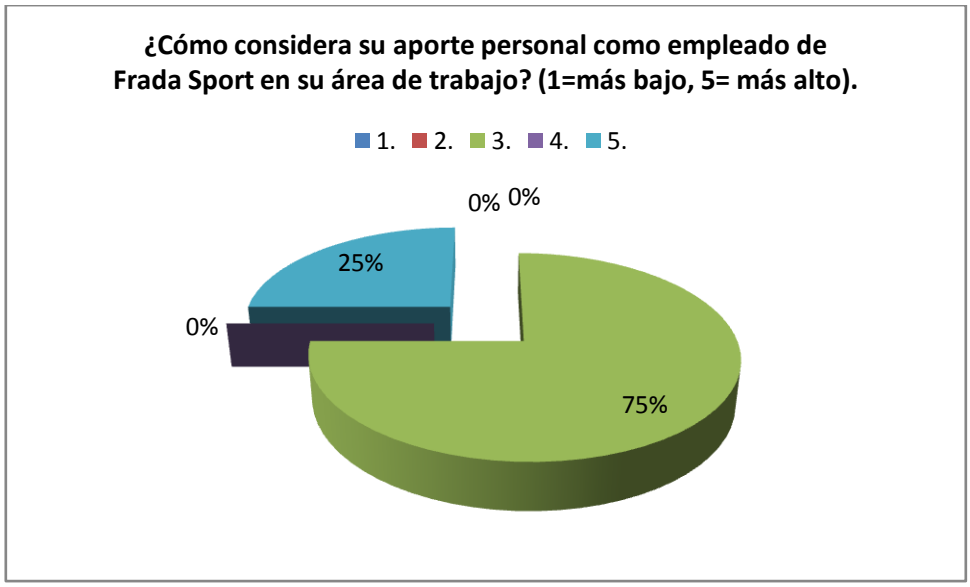


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 50%, considera un buen ambiente laboral en la empresa Frada Sport, un 33% y un 17%, considera un mal ambiente laboral en la empresa Frada Sport.

- **¿Cómo considera su aporte personal como empleado de Frada Sport en su área de trabajo? (1=más bajo, 5= más alto).**

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

RESULTADO	DATOS	PORCENTAJE
1.	0	0%
2.	0	0%
3.	9	75%
4.	0	0%
5.	3	25%
TOTAL	12	100

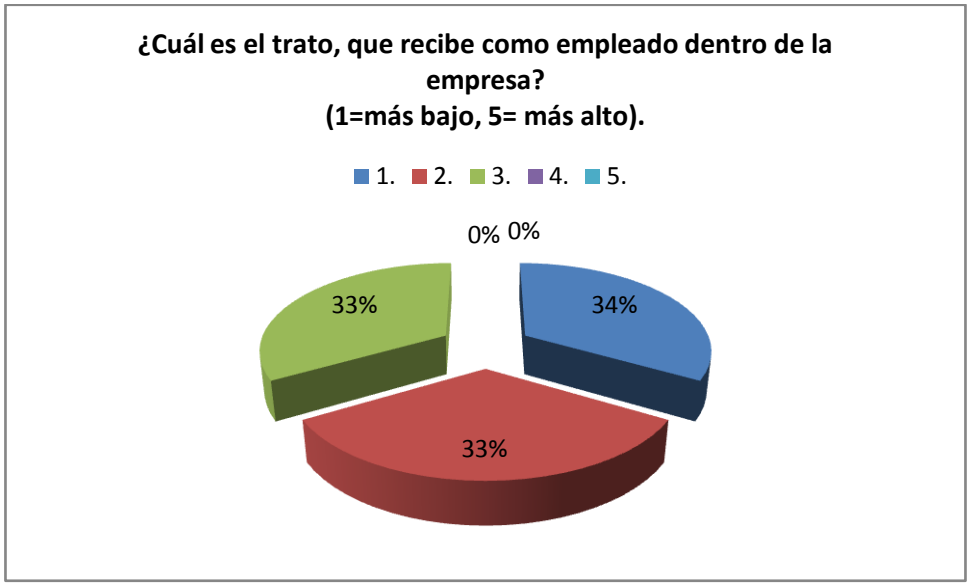


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 75%, considera un buen aporte personal como empleado de Frada Sport en su área de trabajo, y un 25%, considera un mal aporte personal como empleado de Frada Sport en su área de trabajo.

- **¿Cuál es el trato, que recibe como empleado dentro de la empresa? (1=más bajo, 5= más alto).**

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

RESULTADO	DATOS	PORCENTAJE
1.	4	34%
2.	4	33%
3.	4	33%
4.	0	0%
5.	0	0%
TOTAL	12	100%

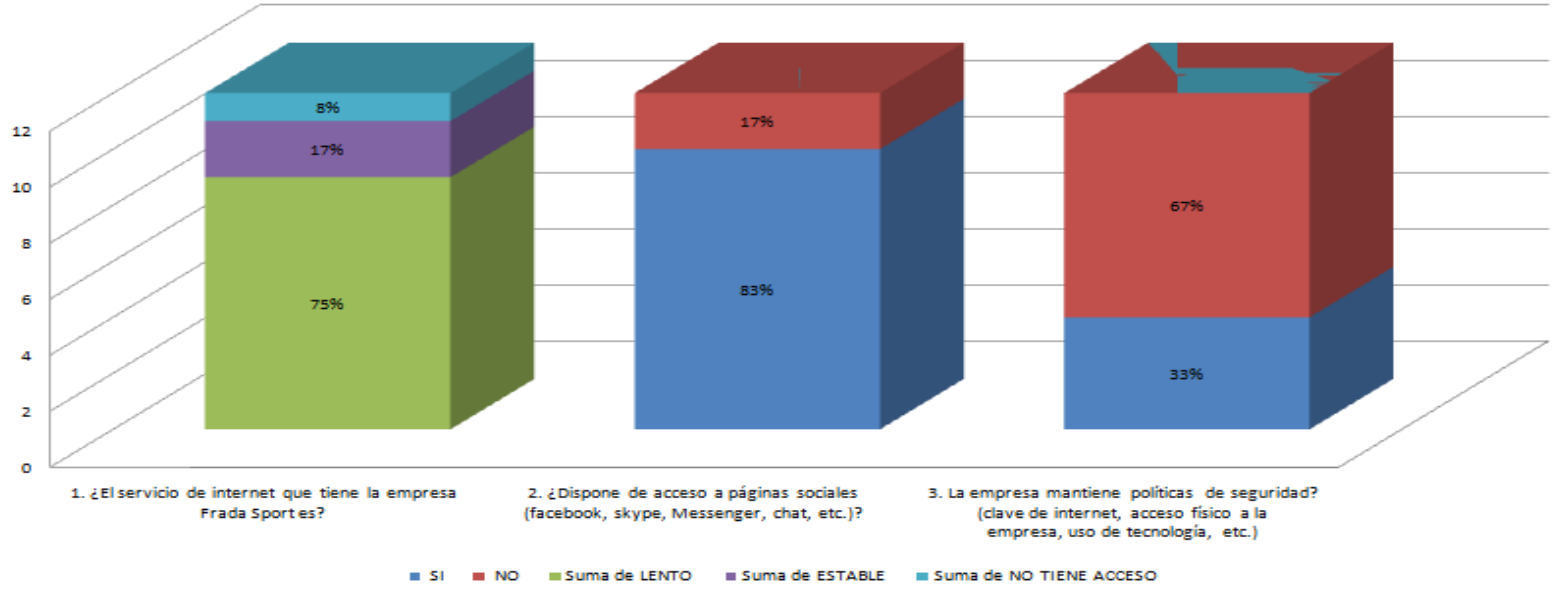


Interpretación.-Para una muestra de 12 personas dentro de la Empresa Frada Sport, se puede determinar que el 34% y 33%, consideran un mal trato como empleado de la empresa, y otro 33%, considera un buen trato que recibe como empleado.

3.10 ANALISIS E INTERPRETACION CRUZADA [9]

GRUPO DE ENCUESTAS, REALIZADO A LOS EMPLEADOS DE LA EMPRESA FRADA SPORT

- **EL internet es muy lento (tráfico en la red)**
  1. ¿El servicio de internet que tiene la empresa Frada Sport es?
  2. ¿Dispone de acceso a páginas sociales (facebook, skype, Messenger, chat, etc.)?
  3. ¿La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)

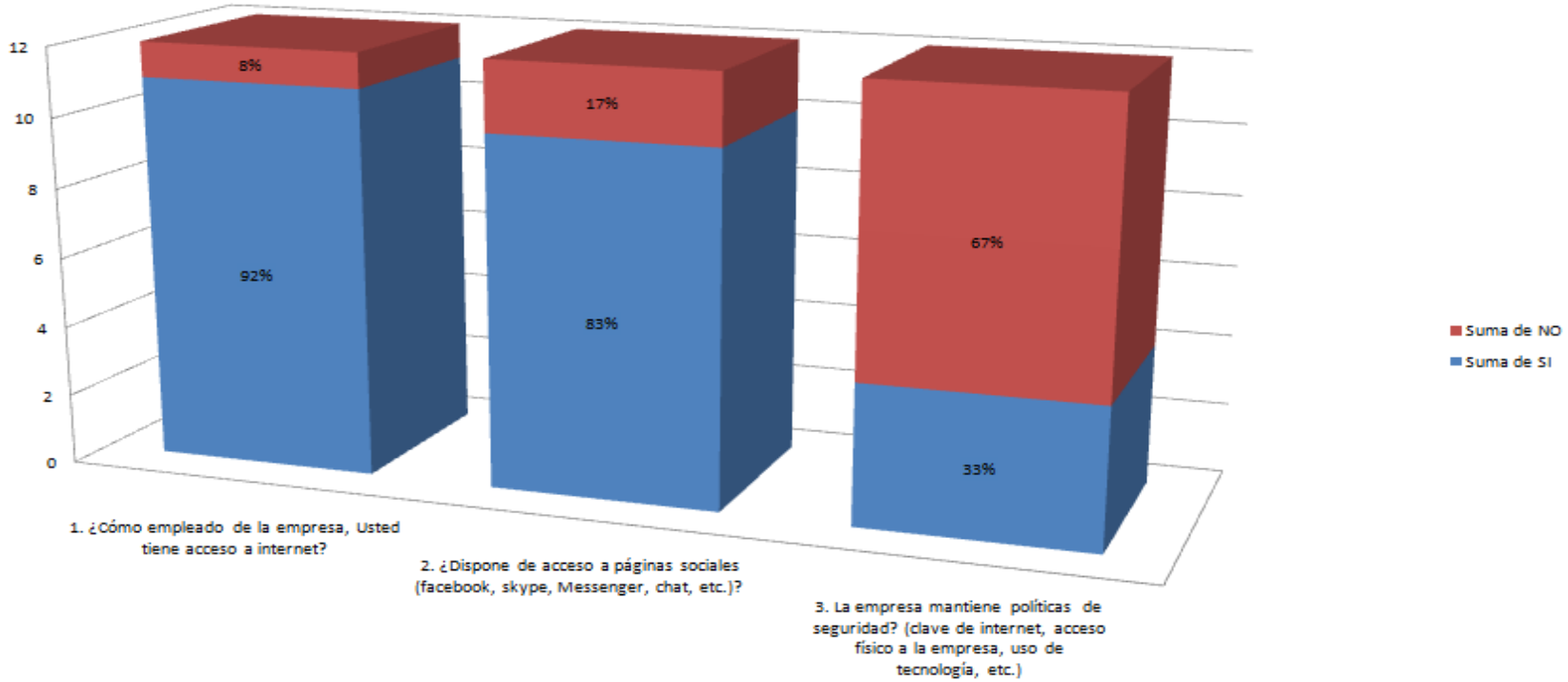


Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que la mayor parte de los empleados (75%), manifiestan que el servicio de internet que tiene la empresa es lenta, debido a que los empleados (83%) poseen acceso a redes sociales como facebook, skype y otros, provocando que en innumerables oportunidades, el internet se vuelva caótico y lento, todo esto, debido a que la empresa no poseen políticas de seguridad (67%).

[9] María Estela Ponce Aruneri, Estadística Inferencial, Mayo 2010.

- **Permitir tener seguridad entrante y saliente de la información**

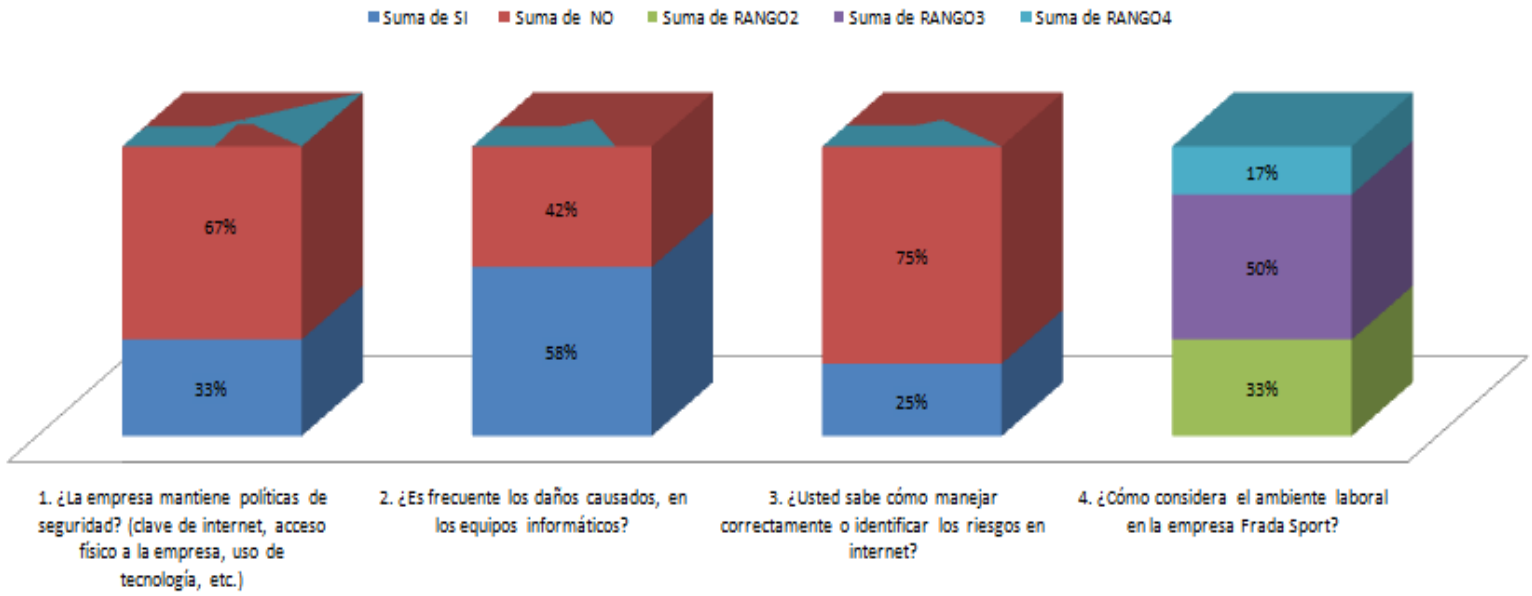
1. ¿Cómo empleado de la empresa, Usted tiene acceso a internet?
2. ¿Dispone de acceso a páginas sociales (facebook, skype, Messenger, chat, etc.)?
3. La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayudará a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que los empleados de la empresa poseen acceso a internet (92%), pudiendo que los datos de la empresa, se filtren o estén en riesgo por medio de internet, por medio de las redes sociales, entre otros (83%), todo esto provocado. Debido a que la empresa no poseen políticas de seguridad (67%).

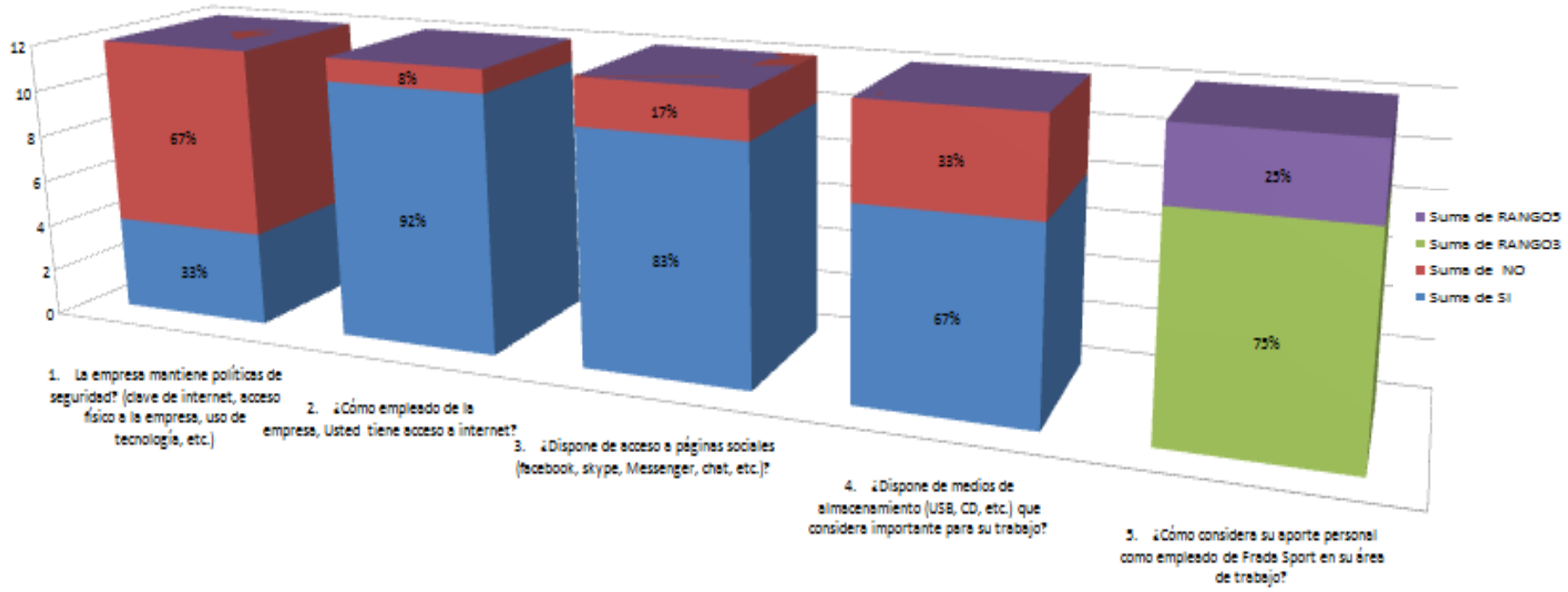
Sistema de Seguridad, abaratando costos

1. ¿La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
2. ¿Es frecuente los daños causados, en los equipos informáticos?
3. ¿Usted sabe cómo manejar correctamente o identificar los riesgos en internet?
4. ¿Cómo considera el ambiente laboral en la empresa Frada Sport?



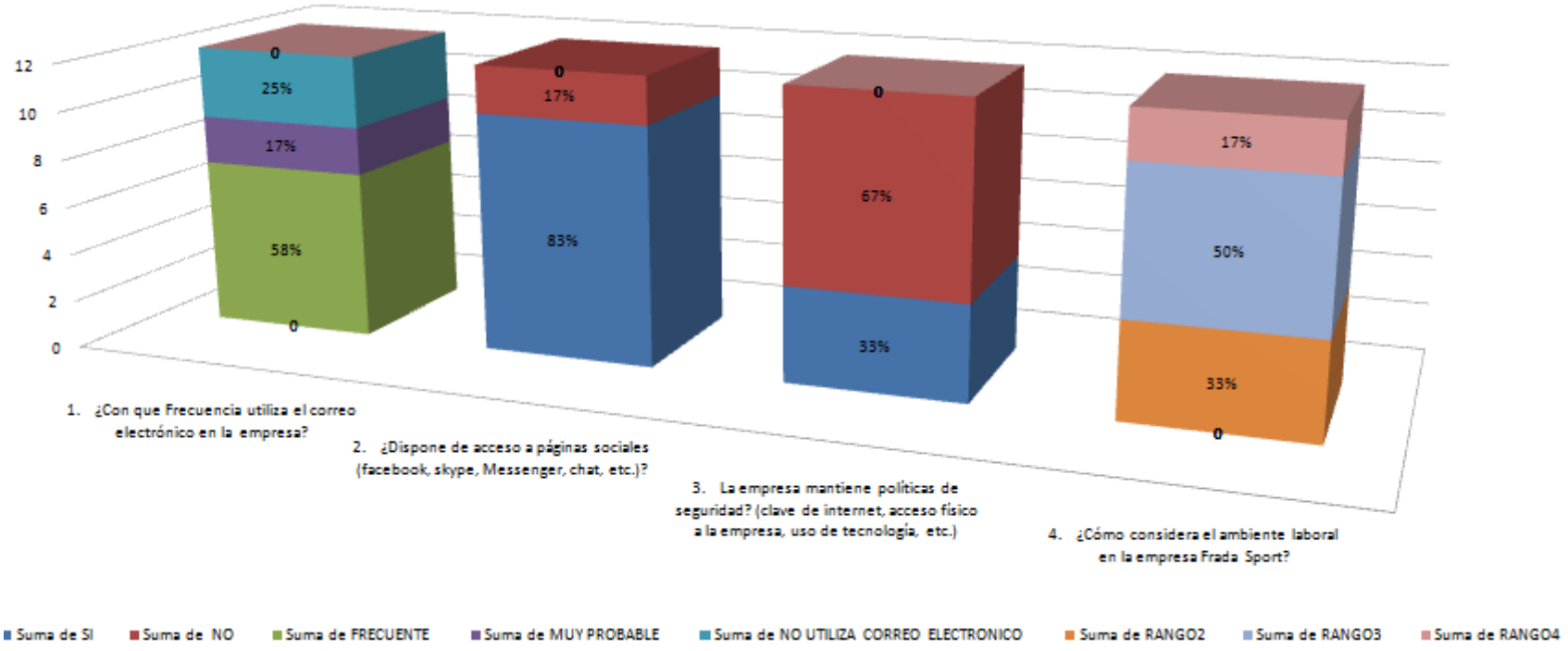
Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que la empresa no poseen políticas de seguridad (67%), es por esta razón que existe daños en los equipos informáticos (58%), producidos por no tener políticas de seguridad, por virus, de no saber cómo identificar correctamente los riesgos en internet (75%), de no poseer ningún sistema de seguridad fiable para la empresa y que le resulte muchos gastos, a pesar de esto, existe un adecuado ambiente laboral en la empresa.

- **Políticas de seguridad**
    1. La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
    2. ¿Cómo empleado de la empresa, Usted tiene acceso a internet?
    3. ¿Dispone de acceso a páginas sociales (facebook, skype, Messenger, chat, etc.)?
    4. ¿Dispone de medios de almacenamiento (USB, CD, etc.) que considera importante para su trabajo?
    5. ¿Cómo considera su aporte personal como empleado de Frada Sport en su área de trabajo?



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar que, la empresa no poseen políticas de seguridad (67%), es por esta razón que tienen acceso a internet (92%) y con a redes sociales dentro de la empresa (83%), además de esto mencionan, que para los empleados de la empresa. Es de vital importancia para la trabajo contar con el acceso a usb, cd, etc. Y finalmente, consideran que el aporte personal como empleados de la empresa es correcto (75%).

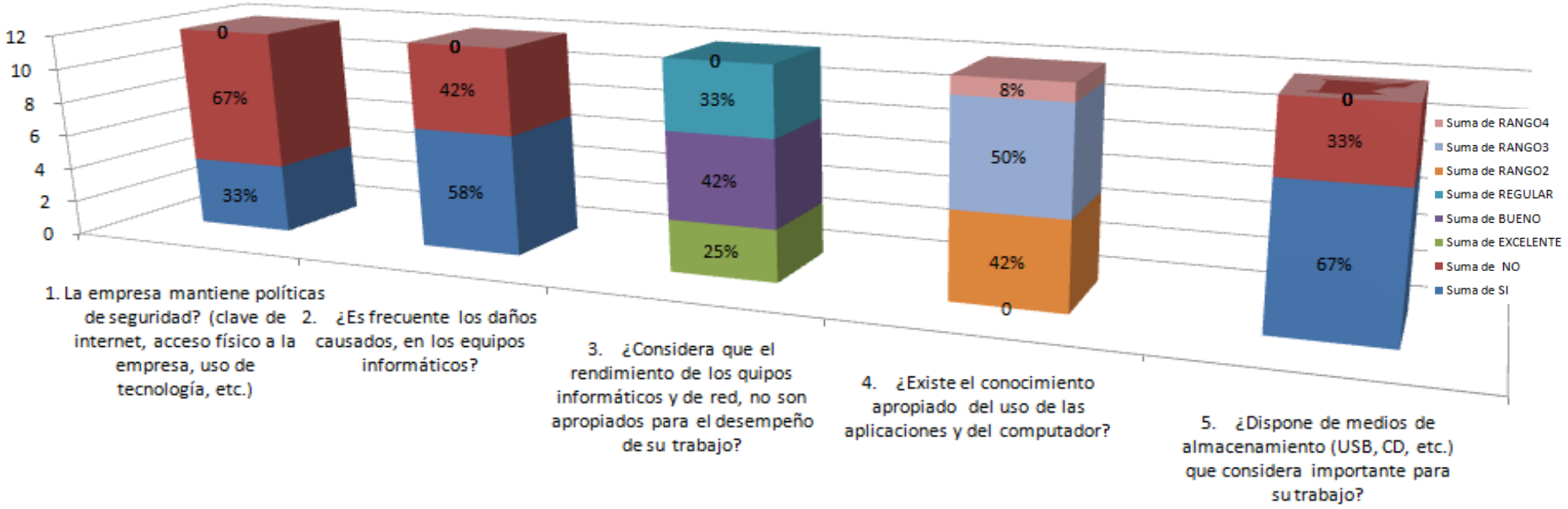
- **Mantener la información confidencial segura, sobre todo los servidores de la empresa.**
  1. ¿Con que Frecuencia utiliza el correo electrónico en la empresa?
  2. ¿Dispone de acceso a páginas sociales (facebook, skype, Messenger, chat, etc.)?
  3. La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
  4. ¿Cómo considera el ambiente laboral en la empresa Frada Sport?



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que el 58%, los empleados de la empresa, utilizan con frecuencia el correo electrónico, esto involucra riesgo, puesto que el correo o en los servidores propios de la empresa, se maneja información de bancos, transacciones, precios, etc, debido también que los empleados poseen acceso a paginas sociales (83%), que involucra un riesgo por el alto nivel de inseguridad, todo esto producido a que la empresa no posee políticas de seguridad (67%), por último, los empleados de la empresa, consideran un ambiente laboral estable.

- **Mejorar el rendimiento de los equipos y de la red**

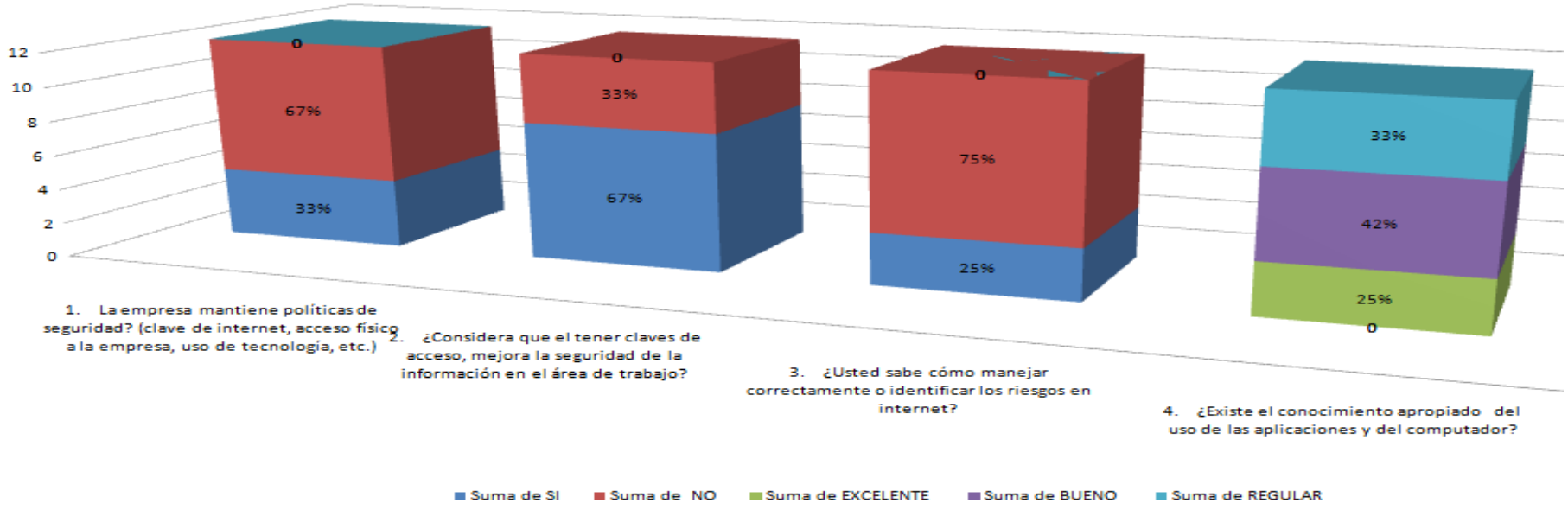
1. ¿La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
2. ¿Es frecuente los daños causados, en los equipos informáticos?
3. ¿Considera que el rendimiento de los quipos informáticos y de red, no son apropiados para el desempeño de su trabajo?
4. ¿Existe el conocimiento apropiado del uso de las aplicaciones y del computador?
5. ¿Dispone de medios de almacenamiento (USB, CD, etc.) que considera importante para su trabajo?



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que la empresa no poseen políticas de seguridad (67%), es por esta razón que por diversos motivos, los daños en los equipos informáticos es frecuente (58%), afectando el rendimiento de los equipos, así mismo, consideran, que el rendimiento de los equipos informáticos y de red, no son apropiados para el desempeño de su trabajo (42%), decir también, que los empleados consideran, que existe el conocimiento apropiado del uso de aplicaciones y del computador (50%), lo que resulta una desventaja, puesto que esta persona, puede manipular, desconfigurar a su conveniencia los equipos, por último, los empleados de la empresa consideran muy importante los medios de almacenamiento USB, Cd lo que resulta un punto negativo para la empresa (67%).

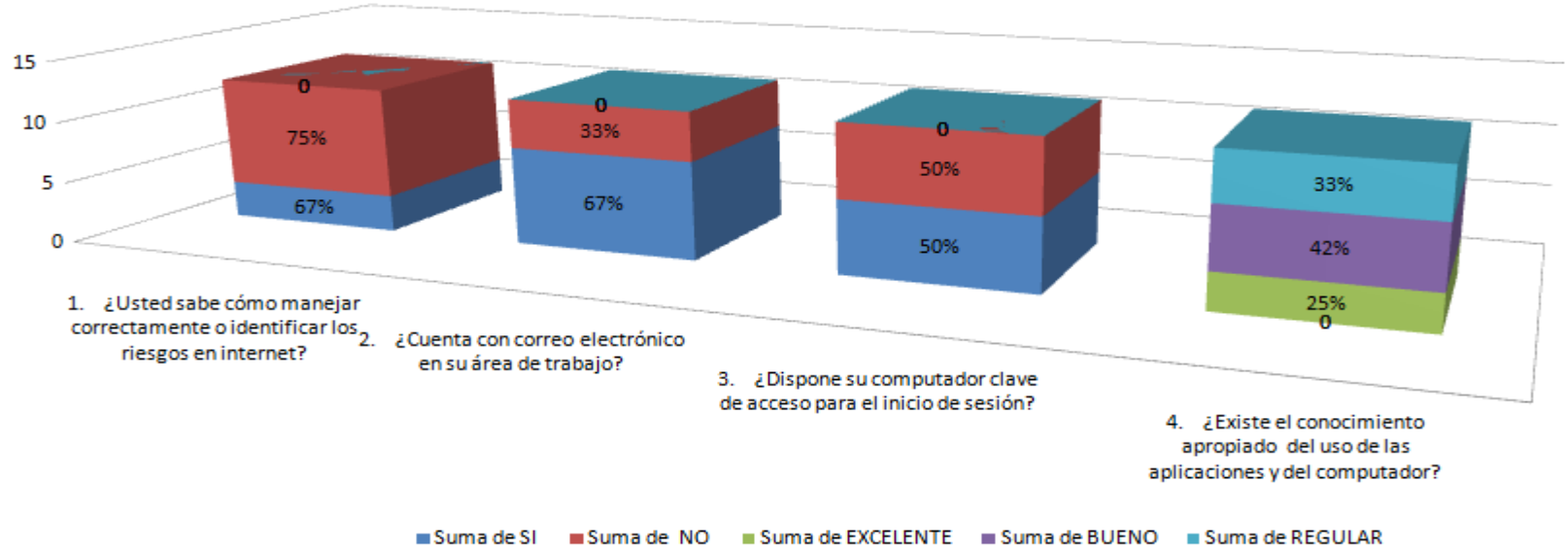
Permitir o denegar el paso de acceso a internet, a los usuarios de la empresa según su área.

1. La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
2. ¿Considera que el tener claves de acceso, mejora la seguridad de la información en el área de trabajo?
3. ¿Usted sabe cómo manejar correctamente o identificar los riesgos en internet?
4. ¿Existe el conocimiento apropiado del uso de las aplicaciones y del computador?



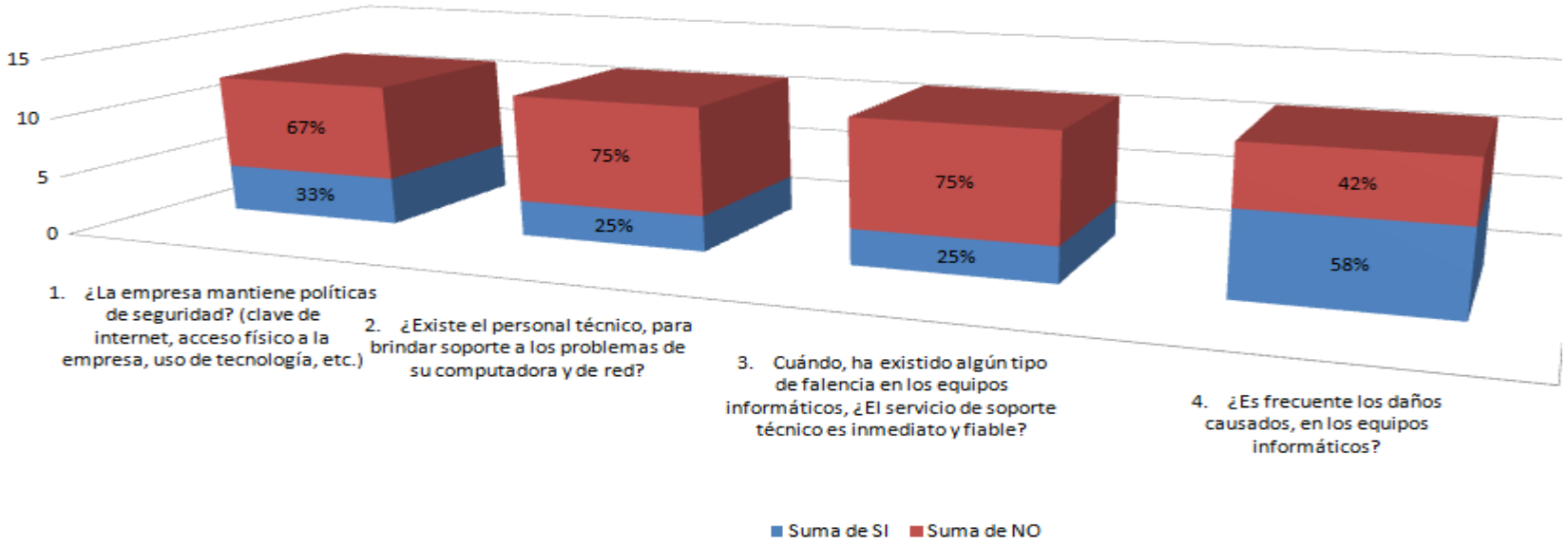
Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar que, la empresa no poseen políticas de seguridad (67%), así mismo, los trabajadores, consideran que el tener claves de acceso, si mejora la seguridad de la información puesto que es ventajoso para la empresa (67%), los empleados mencionan que, no saben cómo identificar los riesgos en internet (75%), este punto es negativo, ya que los usuarios pueden acceder a páginas que filtren la información, que accedan a paginas con virus o correo basura, o que simplemente en horas de trabajo, se dediquen a acceder a webs indebidas por captar mayor interés en otros asuntos que dedicarse a trabajar, así mismo, lo empleados indican que existe el conocimiento apropiado del uso de las aplicaciones y del computador (42%), lo que resulta negativo para la empresa, puesto que pueden manejar a su antojo los equipos informáticos.

- **Tener un control y protección de los datos por medio de un antivirus y anti-spam, métodos inteligentes.**
  1. ¿Usted sabe cómo manejar correctamente o identificar los riesgos en internet?
  2. ¿Cuenta con correo electrónico en su área de trabajo?
  3. ¿Dispone su computador clave de acceso para el inicio de sesión?
  4. ¿Existe el conocimiento apropiado del uso de las aplicaciones y del computador?



Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar, que los empleados, no saben cómo manejar correctamente o identificar los riesgos en internet (67%), así mismo, los empleados cuentan con correo electrónico, y además de esto, no disponen de clave de acceso para el inicio de sesión (67%), todo este grupo de respuestas, generan que el usuario, no tenga una protección global en lo que hace referencia a un control de antivirus que incorpora un firewall, así mismo cada usuario, por medio del internet, genera cada cierto tiempo correo basura, lo que provoca, que el internet se cuelgue repetidas veces, que no acceda a ciertas, etc. Por último, los empleados indican que, existe el conocimiento apropiado del uso de las aplicaciones y del computador (42%), lo que genera un punto negativo, puesto que el usuario cambia, modifica, borra, desconfigura los equipos informáticos, por lo que la empresa, necesita un control centralizado de antivirus, control spam, para que ayude al mejor rendimiento y prevención de infección o correo basura en lo equipos.

- **Documentar toda la información que pasa a través de la red, permitiendo tener un mayor control y organización de los datos en la red.**
  1. ¿La empresa mantiene políticas de seguridad? (clave de internet, acceso físico a la empresa, uso de tecnología, etc.)
  2. ¿Existe el personal técnico, para brindar soporte a los problemas de su computadora y de red?
  3. Cuándo, ha existido algún tipo de falencia en los equipos informáticos, ¿El servicio de soporte técnico es inmediato y fiable?
  4. ¿Es frecuente los daños causados, en los equipos informáticos?



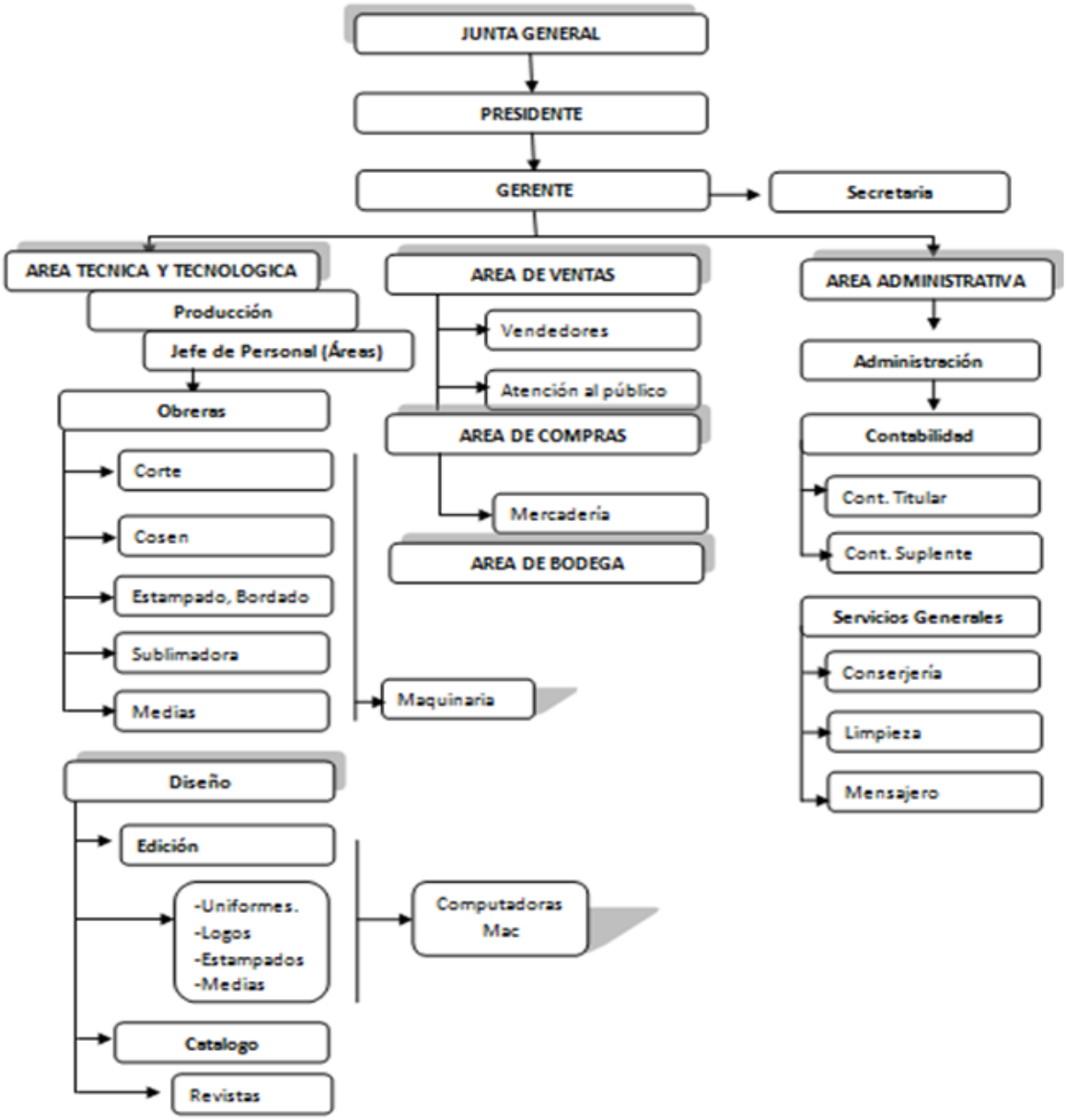
Interpretación.- Para una muestra de 12 personas dentro de la Empresa Frada Sport, se ha desarrollado el presente cuadro que ayuda a la toma de decisiones para obtener el presente resultado de la siguiente manera:
Se puede determinar que, la empresa no poseen políticas de seguridad (67%), así mismo, el personal indica, que es frecuente los daños en los equipos informáticos (58%), por lo que no existe el personal técnico para brindar soporte al computador y al de la red, mencionan también que, el servicio técnico no es inmediato ni fiable, todo esto producido por no tener un control organizativo del flujo de información de la red y de los equipos (75%), ya que los problemas se dan ante la caída del internet, al incorporar nuevos equipos, provocando duplicidad de datos en la red, etc.

CAPÍTULO 4

DESARROLLO

4.1 Antecedentes

ESTRUNTURA GENERAL DE LA EMPRESA FRADA SPORT



4.1.1 Importancia de la Seguridad Informática de la Empresa Frada Sport

Toda la situación, se manifiesta, gracias a los esquemas ineficientes de falta o políticas de seguridad con la que cuenta Frada Sport.

Todo el resultado consiguiente de una "violación" a los sistemas informáticos de la empresa Frada Sport, provoca una inestabilidad y una desorganización, lo que representa un daño con valor incalculable dentro de la misma.

4.1.2 La seguridad informática dentro de la empresa Frada Sport debe basarse en:

1. Integridad de la información.
2. Confidencialidad de la información
3. Alta disponibilidad de los sistemas informáticos
4. Control y Organización de los medios informáticos.

4.1.3 Amenazas y Vulnerabilidades que Presenta la Empresa Frada Sport [10]

Es importante indicar la vulnerabilidad como medio trascendente en la empresa, ya que se establece como la puesta latente de alto riesgo, existe diferentes riesgos en lo que se manifiesta procesos, como:

1. Ataque de virus.
2. Gusanos
3. Mal manejo de la información
4. Spam
5. Nivel de desorganización del flujo de datos en la red.
6. No identificar riesgos

Es primordial tener en cuenta, el crecimiento de la comunicación en Frada Sport, los riesgos va evolucionado y ahora, debe enfrentar a posibles ataques a los servicios o procesos de información, y diferentes amenazas.

[10] Amenazas y Vulnerabilidades: Guillermo Fonseca Ochoa, Amenazas y vulnerabilidades, julio 2012

Por el enorme número de amenazas y riesgos que constantemente corre la empresa, la infraestructura de red y recursos informáticos, debe de estar protegidos bajo un esquema o una normativa de seguridad única, que reduzca los niveles de vulnerabilidad y permita una eficiente administración de riesgo dirigido a los servidores únicos de Frada Sport.

De esta manera, se establece políticas de seguridad, las cuales empieza desde, formar y conocer el manejo de la información, niveles de riesgos, análisis y diseño de la infraestructura operativa y física de la red. Por último, contar con un sistema que brinde o ayude a la empresa de posibles ataques o medidas de vulnerabilidad existente.

4.1.4 Planeación de la Seguridad de la red de la Empresa Frada Sport

El mantenimiento de la seguridad de la red, se necesita dar un acceso fácil a los datos por parte de los usuarios con privilegios y restringir el acceso a los usuarios mediante una segmentación de la red en la Empresa.

Se puede mencionar también, en cuanto a la seguridad de los datos, es tarea del administrador, es también, asegurar o prevenir, que la red se mantenga fiable y segura, simplemente, libre de cualquier amenaza.

En esta parte, se define cómo está la estructura, o como funcionan los módulos o llamados métodos inteligentes de alta disponibilidad Endian Firewall, que es lo que permite, entre otros. Los métodos inteligentes se basan en:

- Diagnosticar el tráfico en la red mediante el sistema Endian firewall
- Incorporar un sistema de Seguridad Open Source, abaratando Costos.
- Seguridad entrante y saliente de la información mediante un sistema de seguridad
- Mejorar el rendimiento de los equipos y de la red
- Documentar toda la información que pasa a través de la red, permitiendo tener un mayor control y organización de los datos en la red.
- Tener un control y protección de los datos por medio de un antivirus y anti-spam, métodos inteligentes.

4.2 Estructura de la Red de la Empresa Frada Sport (Ancho de Banda de 3Mb)

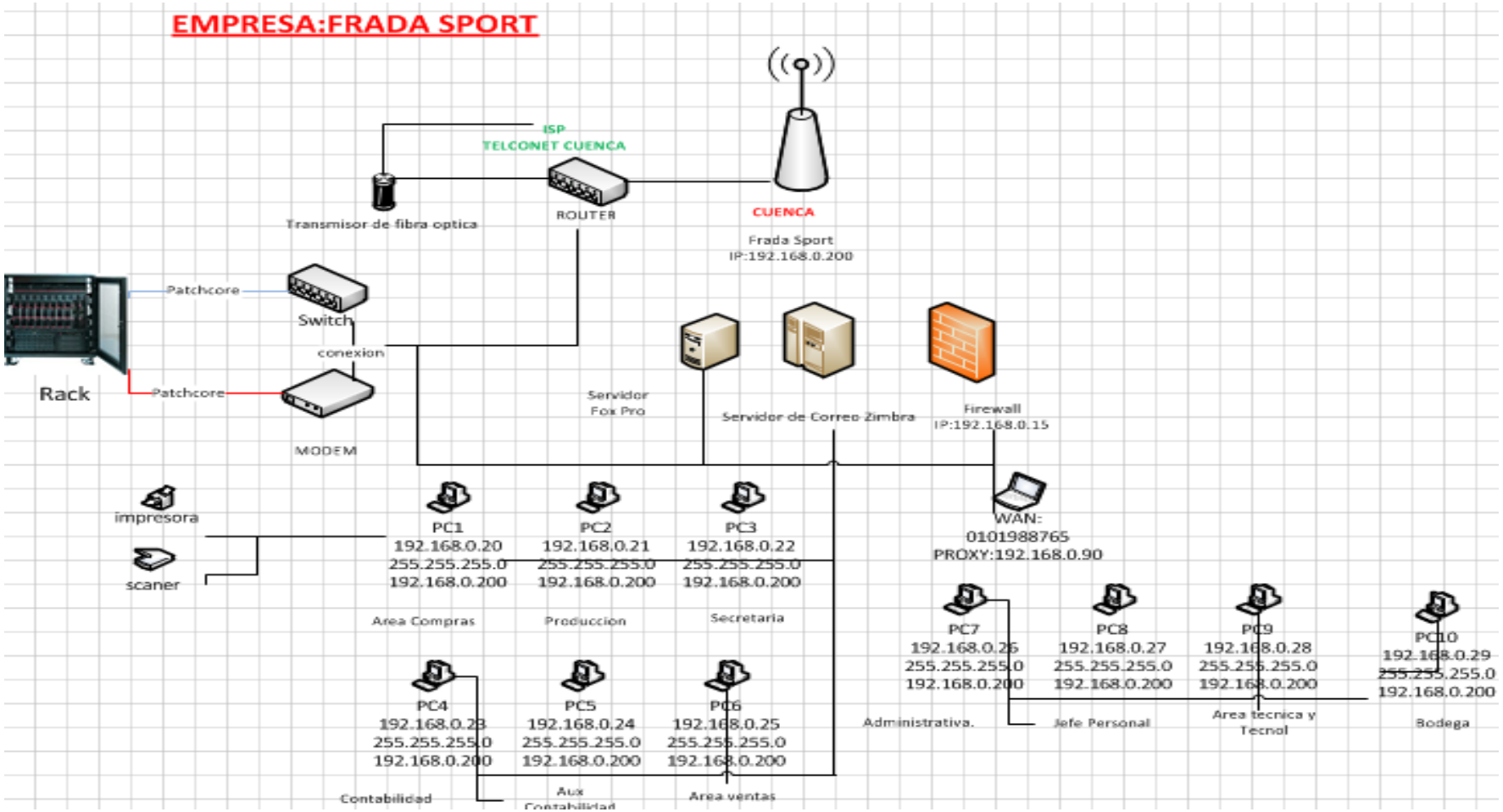


Imagen n°2: Autoría propia diseño *Microsoft Visio 2010,* Estructura de la Red

La empresa Frada Sport, ubicada en la ciudad de Cuenca, está estructurado según el nivel de red, de la siguiente manera:

Posee un rack central, en el cual, esta interconectado con un switch de 24 puertos, un modem y el router que lo proporciona Telconet como su ISP, la señal de su ISP, llega a su router central con fibra óptica, en donde llega la señal de internet a la empresa Frada Sport, el modem a su vez esta interconectado con los patchcore, distribuidos a todas las áreas de la empresa, en la corresponde:

- Área de Compras
- Área de Ventas
- Área de Producción
- Área de Secretaria
- Área de Contabilidad
- Área de Auxiliar de Contabilidad
- Área de Administrativa
- Área de Jefe de Personal
- Área de Técnica y Tecnológica
- Área de Bodega

Principalmente destaca, la interconectividad empalmado del modem-router a los servidores propios de la empresa, estos son:

- Servidor Fox Pro (Sistema de la empresa Frada Sport: Facturación, Precios, Declaraciones SRI, Cuentas de Bancos, Transacciones, Asientos Contables, etc.)

- Servidor de Correo Zimbra (Cuentas de los usuarios de la empresa Frada Sport.)

El ISP, proporciona, un ancho de banda de 3Mb empresarial, la cual es de alta gama para su correcto funcionamiento y velocidad, el servidor firewall, apunta a la Ip estática, redirigido con la: 192.168.0.15.

Este es el servicio proxy que orienta a las demás computadoras del área a crear políticas, reglas, filtros, a contar con un sistema centralizado de auto detentación de intrusos, control de virus y spam, de obtener una estadística certera de vistas del tráfico en la red, del manejo de conexiones, entre otros.

4.2.1 Análisis y Niveles de Riesgo, Manejo de la Información [11]

Filtración de Información:

1. **Transferencias**: Se manejan en muchas oportunidades de una manera online, se encuentra involucrado cuentas de la empresa como, cuenta corriente de diferentes bancos, lo que genera un punto importante en cuanto a nivel de seguridad en la empresa.
2. **Compras Online:** La empresa Frada Sport, está comprando mensualmente un porcentaje moderado de mercadería, por lo que las transacciones corren riesgo que intrusos afecten al sistema servidor de correo zimbra y al servidor fox pro, debido a que en los servidores, pasa toda la información de compras-ventas nacional e internacional.
3. **Proveedores:** Simplemente con receptar un email y responder a este mensaje, basta establecer un negocio nacional e internacional con el contacto directo de proveedores, todo esto manejado por el servidor de correo.
4. **Cuentas de Bancos:** El servidor de correo zimbra que actualmente maneja la empresa, cuenta todos los datos pertinentes a estados de cuenta, ya sea cuenta de ahorra, de crédito, etc, Lo que implica un alto riesgo, debido a que toda la información confidencial de cuentas de bancos se encuentra alojado en los servidores de la empresa.
5. **Listas de Precios:** La información que maneja la empresa como lista de precios de ropa deportiva, se encuentra alojada en los servidores, esto se expone a que hacker o espías, se vean involucrados en dañar o modificar los datos de la empresa.
6. **Finiquitar Negocios:** El área de gerencia, en uno de sus roles como alto cargo, se involucra en finiquitar negocios nacionales o internacionales, con un mensaje de un correo interno que maneja la empresa como zimbra, basta realizar o finiquitar un negocio.

[11] Análisis y Niveles de Riesgo

4.2.2 Análisis y Niveles de Riesgo, según el área, de la empresa frada sport

- **Área de Compras.-** En esta sección, los niveles o los procesos, el departamento de compras, radica en compras ya sea nacionales o internacionales, lo que implica una interactividad con cuentas, bancos, transacciones, etc. Todos los procesos se realizan también por internet, lo que influye un alto nivel de riesgo para la empresa.
- **Área de Ventas.-** En esta sección, los niveles o los procesos, el departamento de ventas, influye, en que todos los procesos de precios, facturas, que es manejado por un personal que tiene acceso a todo, todo este grupo de información es procesada a través de los servidores propios de la empresa.
- **Área de Producción**.- Área de Jefe de Personal, Área de Técnica y Tecnológica.- Todas estas áreas en sí, tienen bastante parentesco en lo que corresponde a los procesos que se manejan en la empresa, aunque se trabaja de una manera independiente, en sí, estas áreas, tienen acceso total al internet, lo que interviene, correo electrónico, redes sociales, manejo de alto de paginas dinámicas que consumen o elevan el porcentaje de fluidez de los datos, entre otros.
- **Área de Secretaria**.-En esta sección, los niveles o los procesos, es decir, la secretaria, influye en la empresa para poseer un nivel riesgo moderado o elevado, posee el acceso a los cobros, al acceso del internet, etc.
- **Área de Administrativa, Área de Contabilidad, Área de Auxiliar de Contabilidad.-** Todas estas áreas en sí, tienen bastante parentesco en lo que corresponde a los procesos que se manejan en la empresa, aunque se trabaja de una manera independiente, por ejemplo, todos tienen acceso total al internet, sin embargo, la contadora principal, tiene acceso a las páginas del SRI de la empresa, bancos, transacciones, estados de cuentas, proveedores, negocios o finanzas, entre otros. Lo que la contadora auxiliar también lo posee, lo cual no es correcto ni apropiado por el alto riesgo de que sufra o exista vulnerabilidad en los procesos de información.
- **Área de Bodega**.-En esta sección, los niveles o los procesos, es decir, bodega, tiene el control de manejar los procesos de proveedores, del departamento de compras y ventas, sin embargo, este departamento, posee el acceso total al internet, lo que resulta en cierto modo, riesgo para la empresa, ya que no cuenta con un control o personal capacitado para el buen manejo de la información.

4.2.3 Diseño y Análisis de la Situación Actual de la Empresa Frada Sport [12]

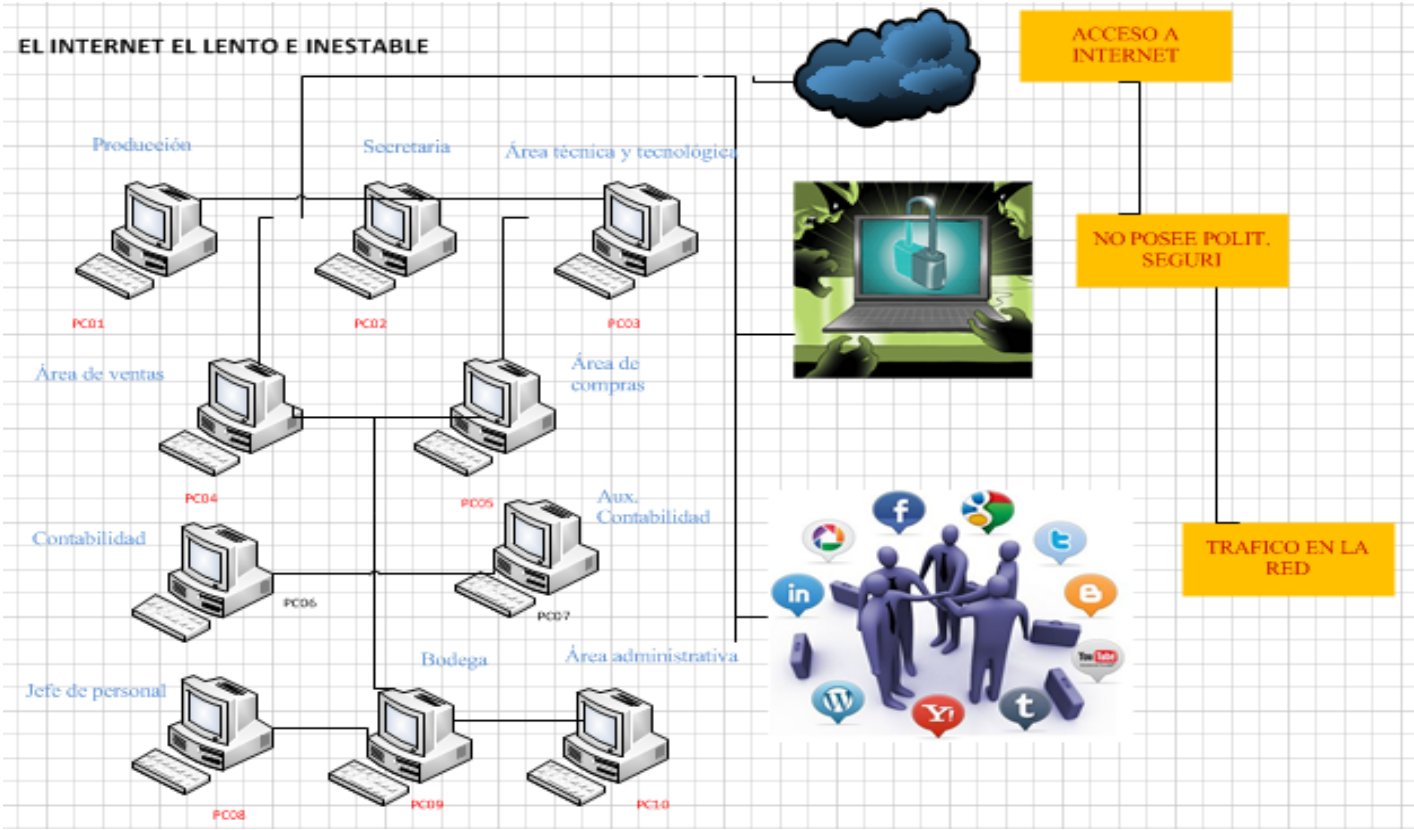


Imagen n°3: Autoría propia Microsoft Visio 2010, Internet Lento

Actualmente la empresa Frada Sport, cuenta con 12 computadoras, que están ejerciendo sus labores en las diferentes áreas de la empresa, sin embargo, mediante las encuestas realizadas al personal, *muestra procesos de configuración y políticas a realizar a 10 computadoras*. Uno de los puntos a desatacar, es que la mayoría de computadores, distribuidas en la empresa, cuenta con acceso total a internet, en la mayoría de los casos, los usuarios, acceden en horas de trabajo a paginas sociales, paginas como facebook, youtube, twiter, etc, todo este contenido de data, almacena gran cantidad de dinamismo en las páginas de internet, lo que provoca que la red se vuelva, lento, caótico, y en algunas circunstancias provoca que el internet se vaya, todo esto originado por que la empresa como tal, no posee políticas de seguridad.

[12] Diseño y Análisis de la Situación actual de la empresa Frada Sport.

4.2.4 Diseño y Análisis de la Situación Actual de la Empresa Frada Sport

(Riesgo de Mantener la Información de la empresa, segura y fiable)

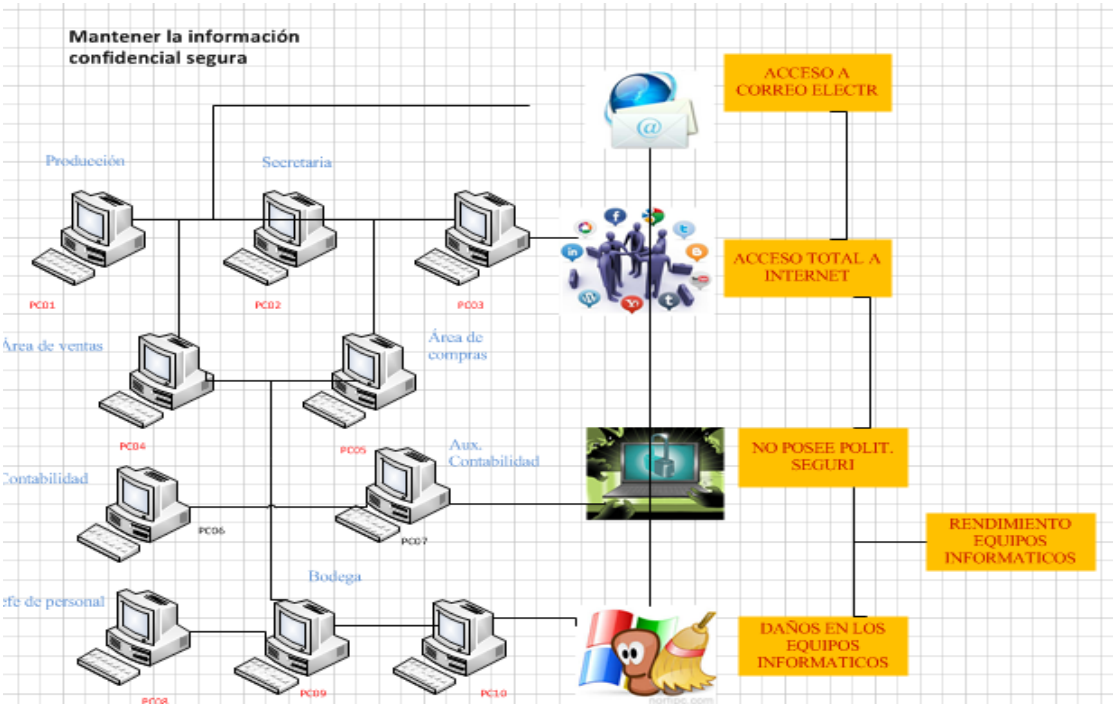


Imagen n°4: Autoría propia Microsoft Visio 2010, Riesgo de la Información

Es importante, tener en cuenta el cómo esta estructura la red en la empresa Frada Sport, se hace referencia, al constante riesgo debido a la alta información de confidencialidad y fiabilidad que maneja la empresa.

Los usuarios de la empresa, poseen acceso al correo electrónico, acceso total a internet, todo esto promovido por no poseer políticas de seguridad, además, el personal como tal, mediante el correo electrónico o páginas como compras, ventas, cuentas de bancos, transacciones, originan un alto nivel de inseguridad a los servidores y a la empresa.

Por poseer acceso total al internet, la data que maneja cada usuario, puede ser violentado, robado por los conocidos hackers, por ingresar a páginas indebidas, originando un mal uso de aplicaciones y del mismo computador o simplemente un riesgo contante para la empresa.

4.2.5 Diseño y Análisis de la Situación Actual de la Empresa Frada Sport

(Rendimiento de los equipos informáticos)

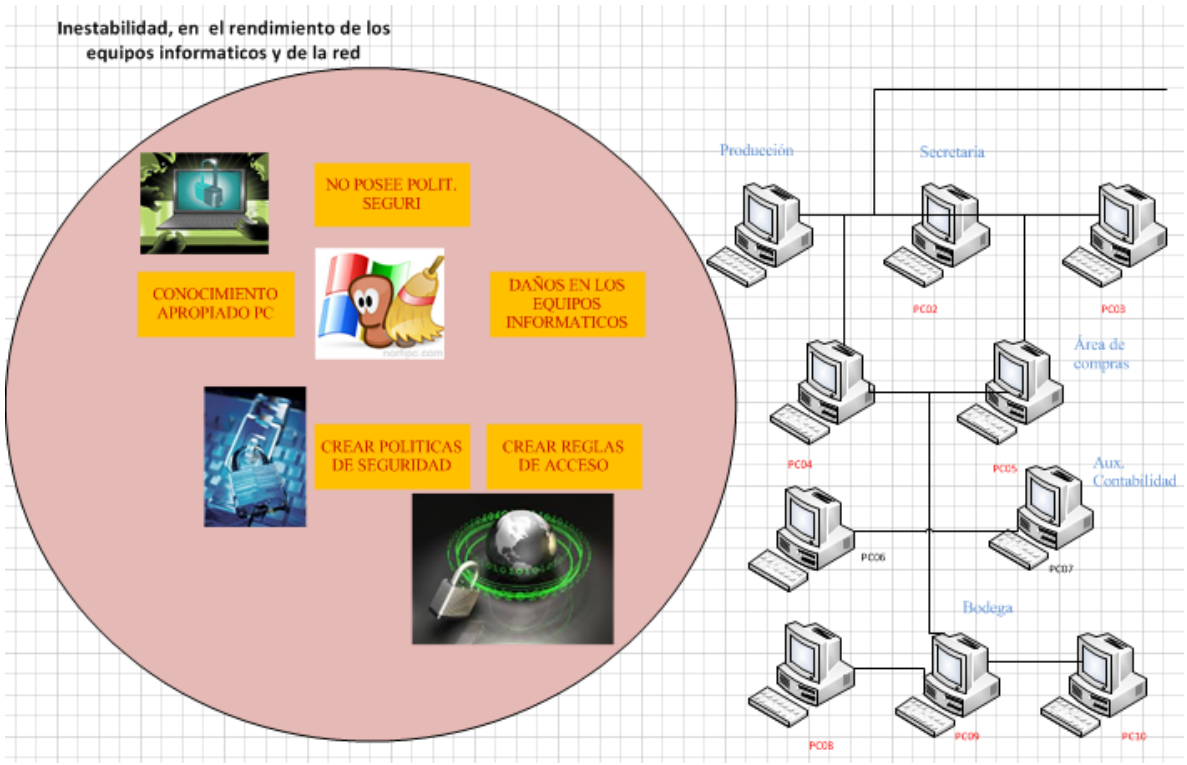


Imagen n°5: Autoría propia Microsoft Visio 2010, Rendimiento de los equipos

Los empleados de la empresa Frada Sport, no poseen políticas de seguridad, lo que influye que muchos de los usuarios, manipulen a su conveniencia las configuraciones, las aplicaciones, el descargarse por medio del internet, contenido malicioso o simplemente virus. Esto se ve involucrado en el rendimiento de software y hardware de los equipos informáticos. En el constante rendimiento y falla de los equipos, muchas son las razones para crear otro nivel de seguridad, que ayude a la estabilidad, al desarrollo de sistemas de seguridad que mejore el control, organización, seguridad y fiabilidad de los diferentes procesos en cuanto al manejo de la información.

4.2.6 Diseño y Análisis de la Situación Actual de la Empresa Frada Sport

(No control centralizado de Protección de Datos)

Antivirus. AntiSpam

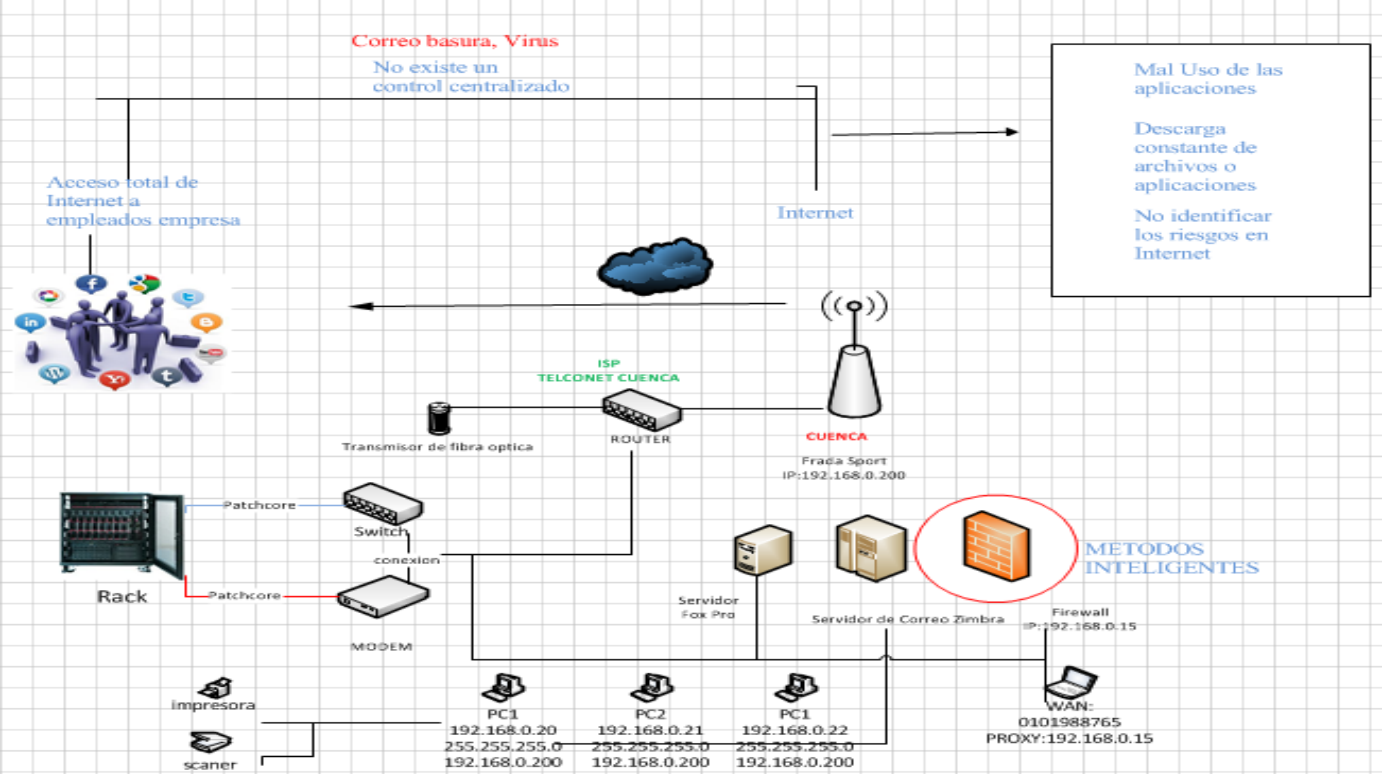


Imagen n°6: Autoría propia Microsoft Visio 2010, Antivirus, Antispam

Representada la imagen número 5, se menciona que, los empleados de la empresa como tal, tienen acceso total a internet, esto involucra un riesgo peligro constante para los datos y apara la empresa, todo este acceso a la nube conocido como internet, genera que los usuarios de la empresa, mediante el manejo a todas las páginas basadas en publicidad, email, redes sociales, entretenimiento, etc, genere una gran cantidad de virus, de información basura, que se manifiesta únicamente, haciendo o provocando daños en el software y hardware, también promovido, por el mal uso de acceso a la nube, a descargar constantemente archivos o aplicaciones, y lo más importante, que en este caso es, la de no saber identificar los riesgos en la web.

4.2.7 Configuración de los Equipos Informáticos de la Empresa Frada sport.

Levantamiento de la Información.

La empresa Frada sport, posee 12 computadores enlazados a la red, el cual 4 equipos de cómputo, se encuentran interconectados mediante DHCP, este flujo de datos, incorpora el ISP, que es TELCONET.

El resto de computadores que son 8 equipos, se encuentran conectados y enlazados con ip fija, proporcionando en este caso el ISP, DNS para compartir conexión establecida a las puertas de internet.

Modelo Sistemático Actual de Configuraciones Dhcp

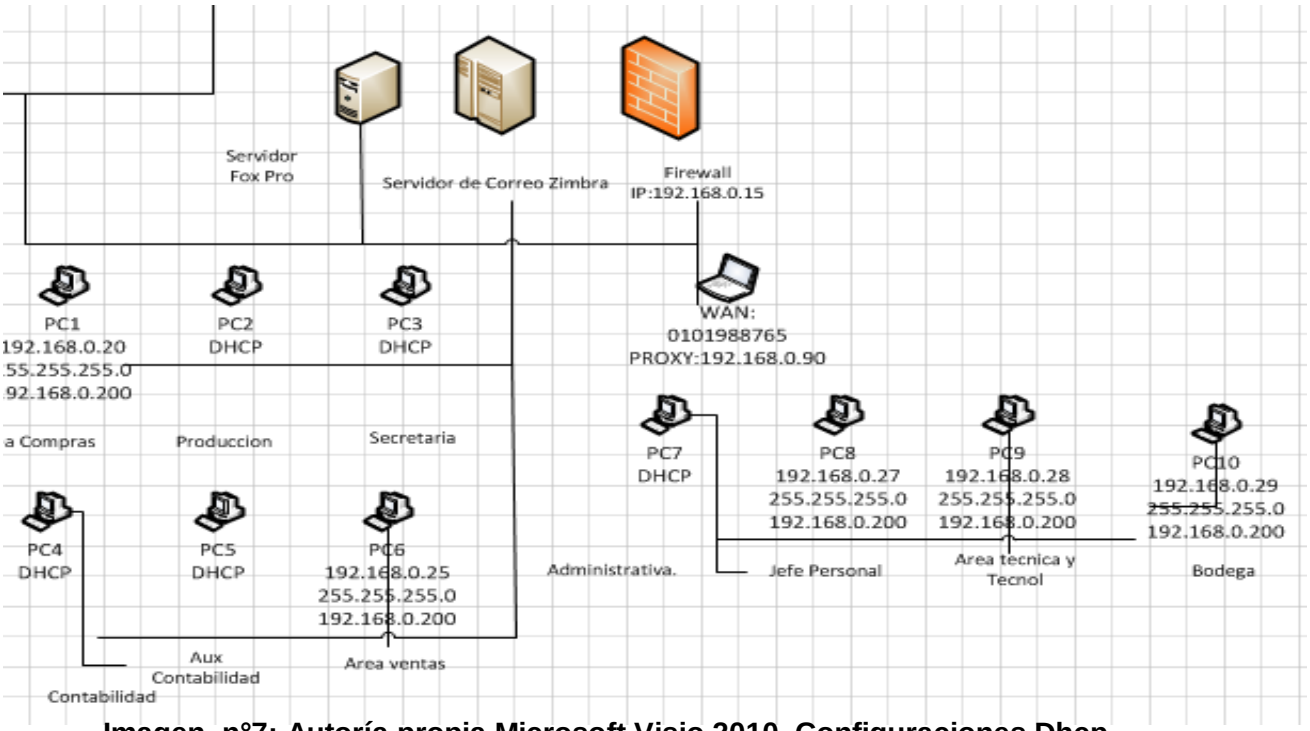


Imagen n°7: Autoría propia Microsoft Visio 2010, Configuraciones Dhcp

El modelo actual que posee la configuración de los equipos informáticos, establece una red de Ip fija y DHCP.

Tales aéreas comprendidas entre:

- Producción
- Secretaria
- Contabilidad
- Auxiliar Contable
- Área Administrativa.

Estas áreas de la Empresa Frada Sport, constituye la red mediante Telconet, brindar una Ip, una máscara y un Dns automáticamente, para dar acceso al sistema o comunicación a la red, o simplemente establecer conexión para los diferentes medios informáticos.

Para la implementación de Endian Firewall, es complejo y tedioso establecer políticas de seguridad, es importante tener en cuenta que la Ip automática, proporciona el ISP y demás componentes siempre va a estar cambiando, por esta razón, es importante la necesidad de establecer medios de comunicación para cada área diferente, es decir, manejar y cambiar, las áreas que tienen o poseen un sistema de red basado en DHCP, modificar por una Ip, una máscara de red y una puerta de enlace estático.

Es de vital importancia, establecer este tipo de comunicación fija, para dar paso a asignar políticas, reglas, filtros a cada área de la empresa.

4.2.8 Modelo Sistemático Actual de Configuraciones Ip Estático

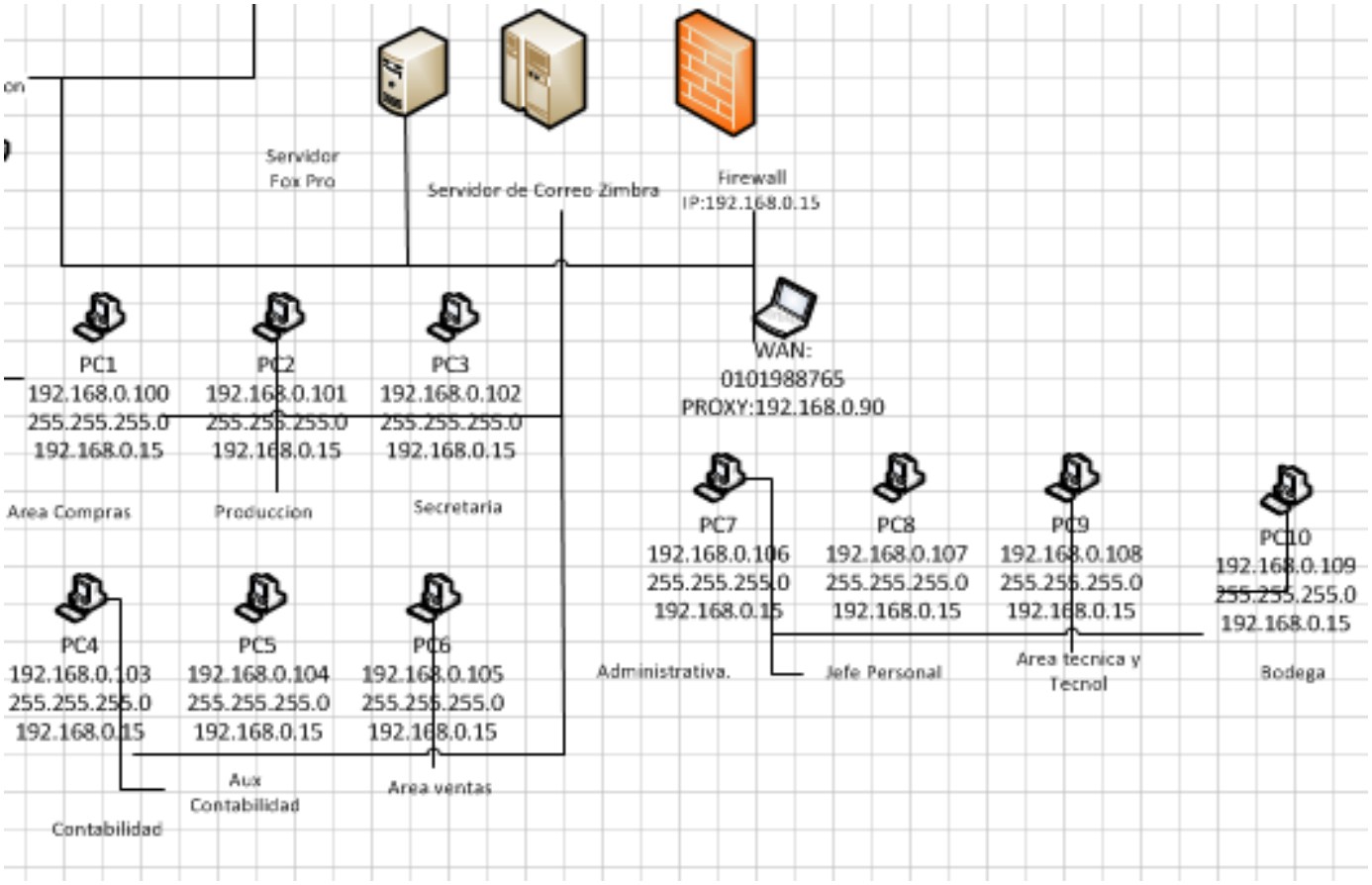


Imagen n°8: Autoría propia Microsoft Visio 2010, Configuraciones Ip Estático

El modelo sistemático, representa un punto primordial para el proyecto, ya que es el punto de partida para poder empezar a emprender el sistema de seguridad.

Es de vital importancia configurar lo equipos informáticos de la empresa de cada área, estas son:

Todas las áreas de la empresa, cuentan con un enlace o conectividad a la empresa o a la red, es decir, cada equipo, presenta una IP, una máscara de red, una puerta de enlace y un DNS, para establecer conectividad entre usuarios y a los servidores.

Es importante tener presente la configuración estática de los equipos informáticos, se procede a crear reglas o políticas de seguridad para la empresa Frada Sport.

4.2.9 CUADRO COMPARATIVO DE LAS HERRAMIENTAS DE MANEJO DEL SISTEMA ENDIAN FIREWALL

SOFTWARE DE UTILIZACION ACTUAL	UTILIDAD	SOFTWARE SIMILAR	UTILIDAD
Endian Firewall	.-Procesos intuitivos de Configuración	**IPCop**	Orientado a casa y SOHO (Small Office / Home Office), funciones básica de seguridad.
Endian Firewall	.-Logs de muestra de reportes de datos	**OpenWRT**	Incorpora puntos de acceso a la red, para empresa pequeña
Endian Firewall	.-Interfaz cómoda, reduce caídas del sistema. .-Seguridad Perimetral	**Vyatta**	Específicamente de virtualización, firewall robusto, hardware pre cargado, maneja filtros de seguridad.
Endian Firewall	.-Mejora el rendimiento y servicios del los equipos, servidores, red. .-Incorporación de filtros, políticas, reglas de seguridad.	**Untangle**	Firewall multifunción, enfocado a empresas pequeñas, maneja filtración web, informes, conmutación automática.
Endian Firewall	.-Administración unificada y centralizada	**pfSense**	Potente cortafuegos, flexible y plataforma de enrutamiento.
Endian Firewall	.-Maneja una BD de anti-spam, anti-virus, Ips y servicios de filtración de contenidos.	**IPFire**	Servidor de seguridad en red, enfocada a pequeñas redes domesticas.

CUADRO COMPARATIVO DE LAS HERRAMIENTAS DE MANEJO DEL SISTEMA ENDIAN FIREWALL

SOFTWARE DE UTILIZACION ACTUAL	UTILIDAD	SOFTWARE SIMILAR	UTILIDAD
Clamav Antivirus	Protección contra páginas con contenido malicioso. Phishing, troyanos, etc.	**ClamWin**	Detección de virus, búsqueda de virus, actualizaciones disponibles.
Trafico entrante y saliente	Manejo de envió, recepción, descarga de información.	**DU Meter**	Medidor del Trafico en la Red, precisa la subida y bajada de data.
Servidor Proxy	Utilizado para segmentar grupo de usuario, permitiendo y bloqueando contenidos.	**Squid: servidor proxy-caché**	Servidor web proxy-caché, funcionamiento proxy almacena páginas web y otros.
Reportes Logs	Muestra en pantalla gráficos de reportes en tiempo real.	**Network Inventory Reporter**	Solución de administración, aplica para inventariar datos en la red.
Prevención de Intrusos	Snort, Seguridad entrante y saliente de información.	**Labs DragonJAR**	Seguridad a penetración y hackeo ético.
SMTP	Control antispam.	**SPAM fighter**	Herramienta para evitar mensajes spam seguro y robusto.

4.3 Metodología en Base a las necesidades de la Empresa Frada Sport

4.3.1 Generalidades

T.A.M.A.R.A: Testeo, Análisis y Manejo de Redes y Accesos[13]

Los procesos destacado en el sustento de un sistema de seguridad endian firewall, facilita mecanismos de que abordan medios de confiabilidad, seguridad en la infraestructura física y lógica de la red de datos, disponibilidad, entre otros.

En consecuencia, se determina un grado mayor de una posible vulnerabilidad o puntos críticos en algunos mecanismos de manejo de la información, lo cual se ha convertido la parte de los diferentes manejos de estructura de datos en la empresa, en la prioridad para la misma.

Por tal motivo, se crea y se sigue una metodología, que se acopla a las necesidades de la empresa en base a diferentes procesos y etapas de desarrollo a seguir, denominada: T.A.M.A.R.A: Testeo, Análisis y Manejo de Redes y Accesos, adicionando a esta metodología, la estructura y modelo de administración basado en la correcta supervisión, vigilancia, y procesos centralizados lógicos de una correcta y eficiente forma de llevar y documentar toda la información de la red en la empresa en un sistema de seguridad open source.

Toda la metodología y administración sustenta la protección basada en mecanismos de seguridad, medios centralizados, políticas y procedimientos de seguridad expuestas para reducir vulnerabilidades y aumentar el performance y rendimiento de software y hardware en los equipos informáticos y de la red.

4.3.2 Objetivo de la Metodología

La metodología, tiene por objeto, que a través del sistema seguridad, minimizar riesgos, vulnerabilidades, posibles ataques o filtración de información, garantizar y salvaguardar procesos y medios de información que se considere valiosa y fundamental para la empresa, centralizar en un solo bloque, zonas de seguridad basado en reglas, y políticas de seguridad, para llegar a formar parte de una red segmentada adoptando normativas de seguridad para obtener mejor rendimiento en los medios informáticos a través de la metodología.

[13] Metodología T.A.M.A.R.A

4.3.3 Explicación de la Metodología

Se tiene en cuenta la seguridad en base a protocolos de comunicación, mecanismos de seguridad y otros fundamentos en redes para emprender la metodología existente basados en la práctica del sistema de seguridad protegiendo y reduciendo vulnerabilidades e intrusos.

Como punto de partida, se identifica la empresa "TAMARA en sistemas particulares y medianos", entiéndase particulares a los empleados que tienen y no poseen acceso a internet, a través de un análisis de la situación actual en base a diseños de diferentes manejos de la información y falta de medios se seguridad, para establecer e identificar por el volumen de información y el número de usuarios o empleados que acceden a la web, también se establece conocer los niveles o manejo de la información basada en niveles de riesgo dependiendo del área de trabajo.

Lo referente al Testeo, involucra medidas de comprobar todo el modelo de desarrollo de la red, basado en administrar de una manera eficiente toda la documentación de la red, basado en conexiones, interfaces, entre otros.

Se identifica, y se estructura etapas y procesos a seguir, basado en la metodología en base a las necesidades de la empresa:

ETAPAS:

ETAPA 1

1.- Incorporación del sistema de Seguridad Open Source, abaratando Costos y medidas de prevención basado en mecanismos de seguridad.

- Sistema de Seguridad, abaratando costos

ETAPA 2

2.- Modelo de administración mediante, control y organización de los datos en la red, basados en subprocesos (sistema, estado, red y registros del endian firewall) de toda la información que pasa a través de la red.

- Documentar todo el sistema de manejo de las redes mediante el Endian Firewall que permita tener un nivel de control y organización para la administración de la red.

ETAPA 3

3.- **Seguridad entrante y saliente de la información mediante un sistema de seguridad**

- Mantener la información confidencial segura sobre todo los servidores con la incorporación de un sistema de seguridad.
- Control Automático, de auto detección de intrusos

ETAPA 4

4.- Control y protección de los datos por medio de un antivirus y anti.spam (métodos inteligentes) centralizados.

- Mantener la información segura durante la entrada y salida de datos a los llamados spyware, hackers.
- Control total de los servidores de la empresa

ETAPA 5

5.-Mejorar el rendimiento de los equipos y de la red

- Mejorar el rendimiento de los equipos y de la red, mediante el acceso y no acceso a internet a los usuarios de la empresa, según el área en que se desempeñan.
- Control y seguridad a la hora de realizar, compras por internet, mediante métodos inteligentes.
- Control organizativo a los usuarios de la empresa, basado en crear políticas de seguridad mediante especificar el tamaño máximo para descargar y subir archivos.
- Crear reglas de acceso, mediante autenticación para cada usuario
- Ver a que paginas ingreso cada usuario (registros. proxy)

ETAPA 6

6.- Diagnosticar el tráfico en la red mediante el sistema Endian firewall

- EL internet es muy lento debido a que múltiples usuarios tiene acceso a internet

4.3.4 (1).- Incorporación del Sistema de Seguridad Open Source, Abaratando Costos y medidas de prevención basado en mecanismos de seguridad. [14]

ETAPA 1 (Anexo 1.1)

- Sistema de Seguridad, abaratando costos

Uno de los requerimientos medidos por la empresa, es generar un sistema fiable, seguro, y que influya en el nivel de control y organización para la correcta administración de los procesos de la empresa y ámbito informático.

Se establece un diseño de la situación actual que representa, el tráfico en la red, el rendimiento de los equipos informáticos y procesos de la empresa, el mantener los datos seguros y fiables, y por último, identificar y establecer un modelo de diseño, que permita saber cómo está estructurada la red en la empresa Frada Sport.

Instalar en el servidor de Correo Zimbra, otro servidor, que es en este caso Endian Firewall, ya que posee un sistema CentOs vs 5.8.

Esto hace, que la inversión se vea reflejado en los contos principalmente, ya que no implica la necesidad de comprar o implementar otro servidor, reduciendo todos los gastos operativos para la empresa.

Basta con el servidor propio de la empresa, que ya se encuentra incorporado, en este caso, el servidor de correo Zimbra, instalar el sistema de seguridad, reduciendo procesos.

[14] Incorporación del Sistema de Seguridad Open source abaratado costos y medidas de prevención

4.3.5 Características de Equipos a configurar (Software, Hardware)

El servidor propio de la empresa, Servidor de Correo Zimbra, cuenta con las características necesarias para emprender un sistema de seguridad open source, cuenta con las características necesarias para implementar en este sistema operativo.

El firewall, representa, características mínimas de instalación y configuración, tan solo con un paquete de 250 Mb, se procede a incorporar en la empresa un sistema único de control y seguridad fiable para toda la red global de datos.

Área	**IP/PUERTA ENLACE**	**Destinatario**	**Especificaciones Técnicas (hardware)**	**Características de Configuración (software)**
Servidor Endian Firewall	**192.168.0.15**	**Empresa Frada Sport**	Mainboard: D945GCNL: BTNL73500A9F Memoria: Value select 4gb serie: B667D2 Disco Duro: Maxtor 250 Gb serie: 5ra5xw3w Procesador: Intel Core I5 2.3 Ghz. Monitor: MONITOR AOC 718SWAG-1	• Endian Firewall: • Sistema, estado, red y registros endian firewall • Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad • Tráfico entrante y saliente
Área de Compras	Pc8 192.168.0.107 192.168.0.15	Sr. Pedro Rodríguez	Mainboard: P4M900: EWD79004 Memoria: MEGA12082 1GB C/U Disco Duro: Disco Maxtor 120 GB Procesador: INTEL CORE 2 DUO 2.4GHZ Monitor: MONITOR AOC 718SWAG-1 Impresora: EPSON LX 300+II SERIE: GDBY2970057	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.

Área de Ventas	Pc6 192.168.0.105 192.168.0.15	Sr. Juan Orozco	Mainboard: BIOSTAR P4M 800-M7 Memoria: KINGSTON: 1 GB Disco Duro: HITACHI 0A38018 320 GB Procesador: Core 2 duo 2 ghz Monitor: AOC H2484JA028177 Impresora: LX 300+II G8DY274389, LEXMARK X75 04260247943	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área de Producción	Pc6 192.168.0.101 192.168.0.15	Lcdo. José Padilla	Mainboard: DG41RQ intel core 2 duo 001cc0egec82 Memoria: KINGSTON: 1 GB Disco Duro: HITACHI 0A38018 320 GB Procesador: Core 2 duo 2 ghz Monitor: AOC H2484JA028177 Impresora: LX300+ETUY277485	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área de Secretaría	Pc3 192.168.0.102 192.168.0.15	Sra. Miriam Fajardo	Mainboard: BIOSTAR P4VMA Memoria: 1GB KINGSTON Disco Duro: SAMSUNG 80 GB Procesador: CELERON 2.8GHZ Monitor: SAMSUNG HA17H9NYA09872A Impresora: LX 300+ ETUY182520	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área de Contabilidad	Pc4 192.168.0.103 192.168.0.15	Ing. Luis Chasi	Mainboard: DG841RQ: 0027DE2E5C7F Memoria: 2Gb de Ram KINGSTON Disco Duro: WESTER DIGITAL :WCATR1756148 500GB Procesador: PENTIUM DUAL CORE Monitor: AOC 7185WAG-1 Impresora: LX 300+II G8DY214547	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.

Área de Aux Contabilidad	Pc 192.168.0.104 192.168.0.15	Ing. Pedro Delgado	Mainboard: INTEL D945GCPE AAD97209201 Memoria: KINGSTON: 1GB F9905316 005A0 4LF Disco Duro: SAMSUNG 52DFJ9C2901146 500GB Procesador: Dual Core Monitor:Samsung, s6nsk2wsa Impresora: Hp	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área Administrativa	Pc7 192.168.0.106 192.168.0.15	Ing. Pedro Bonilla	Mainboard: Intel core i5 Memoria:4 ram Disco Duro:500 Gb Procesador: Intel core i 5 Monitor: AOC Impresora:Hp	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área Jefe de Personal	Pc1 192.168.0.100 192.168.0.15	Ing. Luis Chávez	Mainboard:Intel 28jdl39k Memoria:4Gb Ram Disco Duro:Maxtor 500 gb Procesador:Inter core i3 Monitor: Samsung Impresora: Lexmark	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.
Área de Bodega	Pc10 192.168.0.109 192.168.0.15	Sr. Juan Quinde	Mainboard: Celeron 2.6 Memoria: 500 Mb ram Disco Duro: 120 GB Procesador: Celeron 2.6Mhz Monitor: Samsung Impresora: LX 300+II	• Clamav Antivirus • Snort (Ips) • Segmentación de la Red, Políticas de Seguridad. • Tráfico entrante y saliente.

4.3.6 Detalles Endian Firewall Características Software Hardware

	Características del Hardware					Características en Software	
General	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Número sugerido de usuarios	N/A	<25	<100	<250	250+	5-10	25+
Soporte directo de ENDIAN	x	x	x	x	x	x	x
Seguridad en la Red	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Firewall	X	X	X	X	X	X	X
Prevención contra intrusos (Snort)	X	X	X	X	X	X	X
Múltiples IPs públicas	X	X	X	X	X	X	X
Manejo de la calidad de servicio y ancho de banda	X	X	X	X	X	X	X
Soporte SNMP	X	X	X	X	X	X	X
Soporte VoIP/SIP	X	X	X	X	X	X	X
Escaneo de puertos	X	X	X	X	X	X	X
Prevención de flujos SYN/ICMP	X	X	X	X	X	X	X
Protección contra suplantación de identidad	X	X	X	X	X	X	X
Seguridad Web	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Proxies HTTP & FTP	N/A	X	X	X	X	X	X
Anti-virus	N/A	X	X	X	X	X	X
Soporte transparente del proxy	N/A	X	X	X	X	X	X
Análisis y filtrado de contenidos	N/A	X	X	X	X	X	X
Autenticación: Local, RADIUS, LDAP, Directorio activo	N/A	X	X	X	X	X	X
Seguridad de Correo	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Proxies SMTP & POP3	N/A	X	X	X	X	X	X
Auto aprendido de Spam	N/A	X	X	X	X	X	X
Reenvío de correo transparente (BCC)	N/A	X	X	X	X	X	X

X= Si, x= Opcional, N/A = No Aplica

Imagen n°9: Detalles software, hardware Endian Firewall

4.3.7 Alta Disponibilidad en la Red de Datos

La empresa Frada Sport, utiliza la infraestructura de alta disponibilidad mediante el sistema de seguridad de alto rendimiento (firewall), para proporcionar una ventaja competitiva y tecnológica, aumentar la productividad, y la autonomía de los usuarios dependiendo su área de trabajo. Es más rápido tomar decisiones y llevar un control de acuerdo a las necesidades de la empresa.

Sin embargo, los beneficios ha llegado una dependencia cada vez mayor de la infraestructura. Si una aplicación o mal manejo de la información, basada en su mal uso, entonces toda la empresa puede estar en constante riesgo. Los ingresos, los clientes, los sistemas de control, las ventas, pueden estar involucrados en constantes falencias en los sistemas, y poder perderse.

Es muy importante examinar los factores que determinan la forma en que los datos son protegidos, y puede en ciertos manejos de la información, ser vulnerables y maximizar la disponibilidad para los usuarios, dependiendo de las funciones dentro de la empresa.

4.3.8 Alta Disponibilidad, Se mide en Diferentes Procesos de Manejo, basado en:

Fiabilidad: Los componentes, hardware, identifica la fiabilidad de una solución del correcto manejo, el software seguro, incluida procesos de desarrollo, servidores fox pro, servidor de correo y aplicaciones, es la parte crítica de la implementación de la solución de alta disponibilidad.

Si bien es posible que se pueda recuperar rápidamente dependiendo de las falencias, procesos de información, y del personal técnico que cuente, si el tiempo en solucionar dicho problema, excede en un tiempo determinado, entonces no se puede satisfacer la necesidad de alta disponibilidad. La seguridad de la empresa, depende del entorno de trabajo de acorde a la necesidad única, para ver de forma rápida y notificar sucesos reales minimizando errores y corrigiendo a tiempo.

4.3.9 Protección en la red entrante

Este medio de protección, orienta un mecanismo de acción en lo que hace posible minimizar los riegos en la red de datos en la empresa, es decir, hace que la red no quede inoperable o que los sistemas o medios de informáticos se vean afectados o sufra indistintos daños, tomando en cuenta que la solución optima efectuaría acciones rápidas sin demoras de tiempo determinado.

Se hace referencia a las medidas de soluciones óptima:

- Prevención
- Detección
- Recupera

Como punto de partida, hace referencia a los medios de **prevención**, que reduce notablemente las acciones previas a un ataque determinado, esto hace que aumente el nivel de seguridad de la red en procesos de funcionamiento.

Cuando en la red de datos, pasa información cifrada, rápidamente, mediante filtros, la **detecta**, intentos de filtración de información o amenazas dadas, y finalmente **recupera,** o bloquea los diferentes medios de información en donde se esté dando los diferentes procesos de secciones óptimas en la red global de datos.

4.3.10 Mecanismos de prevención de la red de datos

Nivel de seguridad [15]

El elevado nivel de riesgo que posee la empresa, por la alta confidencialidad de la data, hace referencia a un sistema de red, que depende del entorno en el que trabaja, esta red, almacena y se involucra con una serie de procesos altamente importantes en el nivel de seguridad, basado en:

- Configuración de las políticas normativas
- Prevención
- Autenticación
- Entrenamiento

Equipamiento a nivel de seguridad

Dar un paso primordial, en lo que hace referencia al mantenimiento de la seguridad de los datos, la magnitud de la seguridad depende de:

- ❖ Volumen de la empresa (Frada Sport)
- ❖ Importancia de los datos (nivel de confidencialidad)
- ❖ Medios de recursos disponibles

4.3.11 Seguridad de los servidores

En la empresa, se considera mediana por el volumen y los procesos que se maneja, existe un control centralizado que procesa los diferentes niveles jerárquicos de los datos. En donde existe, gran cantidad de información crítica, uno de los puntos más emergentes y vulnerables de la empresa, es los “servidores”, este es el corazón de los procesos de la información, es importante destacar la seguridad de las constantes amenazas, la cual se basa en encerrar los servidores, con accesos totalmente restringido, a determinados usuarios.

Se encuentran todos los procesos de la empresa como Fox pro, Servidor de Correo Zimbra.

[15] Cristian Guerra C, Nivel de Seguridad, 2011

Permiso de acceso

Representa un modelo de organización y procesos autónomos, con la generación de modelos únicos de prevención.

4.3.12 Ethernet estático o Ip fija

Esta parte es importante, ya que indica los tipos de conexiones, como se indica anteriormente , la red en la Empresa Frada Sport, maneja e incorpora un sistema de IP Fija, basado en establecer Ethernet Estático, para poder crear políticas de seguridad, en este caso, se asigna el Ethernet estático que representa los diferentes módulos de configuración, dependiendo del tipo de necesidad que represente para la empresa, se puede establecer o generar modelos de desarrollo basados en Dhcp, puerta de acceso, entre otros.

Para la empresa Frada Sport, establece la necesidad de configurar y crear políticas de seguridad basadas en Ips fija, es por esta razón que implementa o configura la Ethernet estática.

Se adapta la opción naranja, para establecer el segmento de red accesible para los usuarios de internet, es decir, se genera otro tipo de servidor interno basado en configurar e instalar un server DMZ como punto de acceso a los usuarios de la empresa, para poder ingresar a la Lan interna, y por medio de esta, a la wan como medio de acceso a internet dentro de la empresa.

Se genera y establece las configuraciones previas e ingresado al sistema como tal, como punto de partida, se muestra en pantalla inicial del servidor de seguridad Endian Firewall, en la que se Redirecciona la Ip segura, basada en:

- 192.168.0.15:10443.

Entre los accesos establecidos mediante las necesidades de la empresa, se destaca:

0) HTTP
1) WWW
2) SMTP
3) DNS

La DMZ tiene un nivel de protección intermedio en la red. El nivel de seguridad, no es suficiente para almacenar datos críticos de la empresa, sin embargo hace posible conectar las diferentes políticas o medios de accesos a los usuarios de la empresa.

4.3.13 Costos y Beneficios

Implementado ya el Sistema de Control y Seguridad, Endian Firewall, en la empresa como tal, resulta de suma ventaja, ya que uno de los requerimientos y necesidades es, establecer un sistema de seguridad fiable y segura, que no represente un mayor gasto o inversión a dicha empresa.

Se tiene presente, las necesidades y requerimientos de la empresa, se ejecuta un sistema de seguridad, que ayude a la empresa a tener un control y fiabilidad de los procesos de los datos.

Es por esto, que tal sistema de seguridad, no representa ningún gasto operativo, con solo la descarga de Servidor Endian Firewall destacando Open Source, resulta beneficioso para la empresa, es decir, no se paga costos de licenciamiento, nada mas costos de implementación, las cuales no representan ningún costo mayor para la empresa, además es importante la posibilidad de modificar el producto para adaptarse a las posibles necesidades actuales y futuras para la empresa

4.4 (2).-Modelo de Administración mediante, Control y Organización de los datos en la red, Basado en Subprocesos (sistema, estado, red y registros del Endian Firewall) de toda la información que pasa a través de la red. [16]

ETAPA 2

- Documentar todo el sistema de manejo de las redes mediante el Endian Firewall, que permita tener un nivel de control y organización para la administración de la red.

Después de implementar el Sistema de Seguridad EFW, y de configurar los puntos de acceso al sistema, se conoce algunos puntos importantes que se debe de tomar en cuenta, basado en:

4.4.1 Políticas de reglamento

El Reglamento tiene por objeto determinar las medidas apreciadas por la empresa Frada Sport, básicamente, interactúa con técnicas organizativas que estructure y garantice el correcto manejo de los datos en la red, la confidencialidad, integridad y que se encuentre disponibilidad, además para establecer la finalidad de preservar frente a la alteración, pérdida, tratamiento o acceso no autorizado de información indispensable o única dentro de la empresa.

4.4.2 Generalidades

Dentro de la infraestructura de la red en la empresa Frada Sport, no sólo se incluye el diseño e implantación de seguridad de la red, si no también orientada o relacionada, al correcto funcionamiento de la misma.

Se debe conocer cómo resolver los diferentes problemas cuando se presentan, decidir cuándo es necesario expandir o cambiar la configuración de la red de datos, a fin de reunir las peticiones de cambios.

Cuando la red de la empresa, trabaja normalmente, se realiza una serie de mecanismos, basado en herramientas que ayude a los diferentes procesos de la administración de la red, basado en:

[16] Modelo de Administración

- Documentación de la red
- Conocimiento de cómo se comporta la red, a través de sistemas de administración de redes,
- Correctas configuración, basada en la necesidad de la empresa.
- Estados de los Sistemas
- Interfaces
- Entre Otros

4.4.3 El Sistema de Administración de red, tiene por objetivo:

- ✓ Diseño actual y Planificación (recopilación de la información).
- ✓ Manejo de Herramientas de Servicios de Seguridad
- ✓ Administración de la red de datos.
- ✓ Seguridad en la empresa.
- ✓ Administración ante fallos y rendimiento adecuado.
- ✓ Vigilancia
- ✓ Estados
- ✓ Conexiones
- ✓ Estados de Sistemas y de la red

En la correcta administración en la red, se debe dominar los aspectos que permitan definir la red, estructura lo siguiente:

Algunas actividades detrás de la administración de la red incluyen:

- Administración correcta, para ofrecer un correcto rendimiento estable.
- Control de los medios que ofrece el sistema de seguridad, basado en establecer tanto los subprocesos, como el número de usuarios, interfaces, protocolos, proveedores, para no perder la pista de la red.
- Mejorar el servicio y calidad de la seguridad y administración de usuarios, datos que de alto nivel.
- Establecer distintas necesidades a nivel de administración y control de usuarios y de manera global en la empresa, ejecutando diversas herramientas de mejoras, basado en áreas de rendimiento, disponibilidad y seguridad total.
- Vigilar, controlar la utilización de los recursos para que la empresa.

4.4.4 La Administración de la red, Se compone de sub modelos, planteado con el propósito de tener un entorno de trabajo estructurado y fiable. [17]

a. **Modelo de organización.-** Se describe los procesos de la administración de la red, esto es: acciones de supervisión y control.

b. **Modelo de información**.- Basada en la estructura y el almacenamiento de la información de la administración de datos de la red, la cual se almacena en una base de datos establecida en la empresa *(conexiones firewall)*, para automatizar procesos necesarios y otorgar seguridad física y lógica a la empresa.

c. **Modelo de comunicación**.- Dependiendo de la necesidad que requiera la empresa, para las diferentes actualizaciones o mejoras, se toma referencia en base a su configuración de desarrollo.

d. **Modelo de funcionalidad**, Direcciona la herramienta de administración de red basado en la seguridad, que se encuentran en la empresa.

[17] Ma. Eugenia Macías Ríos, Modelo de Administración, 2011

4.5 (3).- Seguridad entrante y saliente de la información mediante un sistema de seguridad [18]

ETAPA 3 (Anexo 2.1)

- Mantener la información confidencial, segura sobre todo los servidores de la empresa, con la incorporación de un sistema de seguridad.
- Control Automático, de auto detección de intrusos

4.5.1 Arquitectura Snort [19]

El Snort proporciona un conjunto de procedimientos que lo convierte en una herramienta de seguridad muy potente para la empresa.

Se destaca la captura del tráfico de red, el análisis y registro de los paquetes capturados y la detección de tráfico malicioso.

4.5.2 Arquitectura básica Snort o Ips

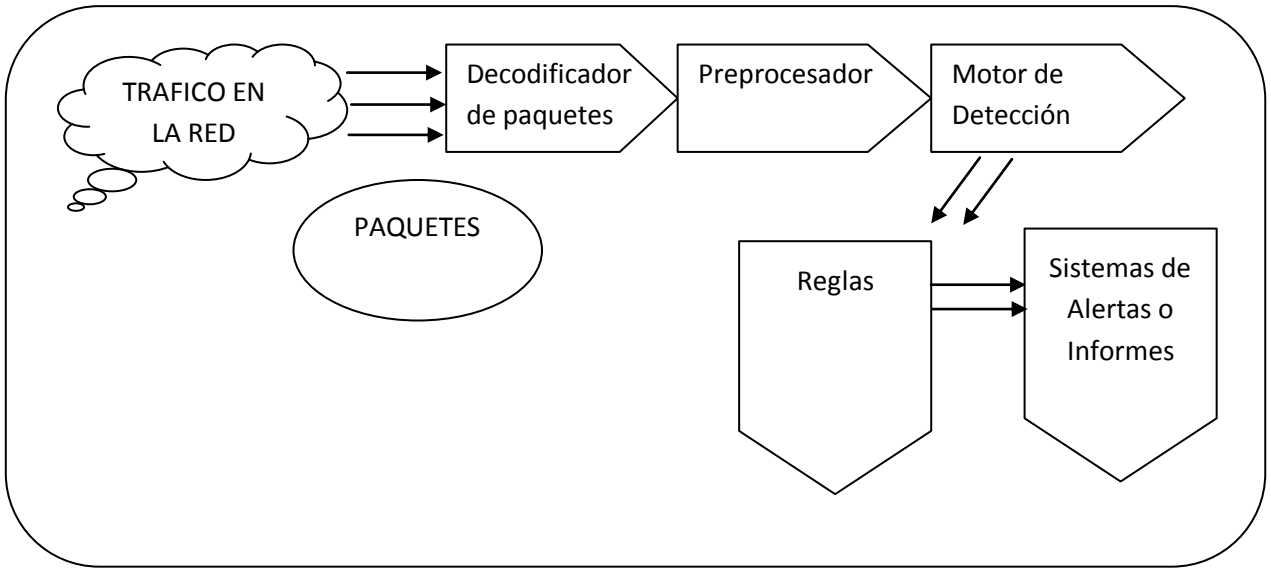


Imagen n°10: Autoría propia, Arquitectura básica Snort

[18] Seguridad entrante y saliente

[19] Joaquín García Alfaro, Arquitectura Snort, 2011

Como actua el Ips o Snort

1.- Recoge paqutes de toda la red gobal de la empresa mediante el trafico en la red.

2.- Ordena todo el grupo de procesos y estructura en forma según la categoria, basado en el motor de deteccion que se mansaje.

3.- El administrador de la red, decide por que reglas se inclina la necesidad de la empresa, para generar posteriormente alertas o informes sobre información maliciola o altalamente compremetida.

4.5.3 Decodificador de paquetes

Lo más importante, es que el decodificador de paquetes de Snort, es el elemento más esencial, encargado de recoger los componentes que más adelante serán examinados y clasificados por el resto de información. Para ello, el decodificador de paquetes debe ser capaz de capturar todo aquel tráfico global y escanear para verificar posibles peligros para la empresa.

4.5.4 Preprocesador

Verifica o escanea puertos de acceso.

Acciones preprocesador

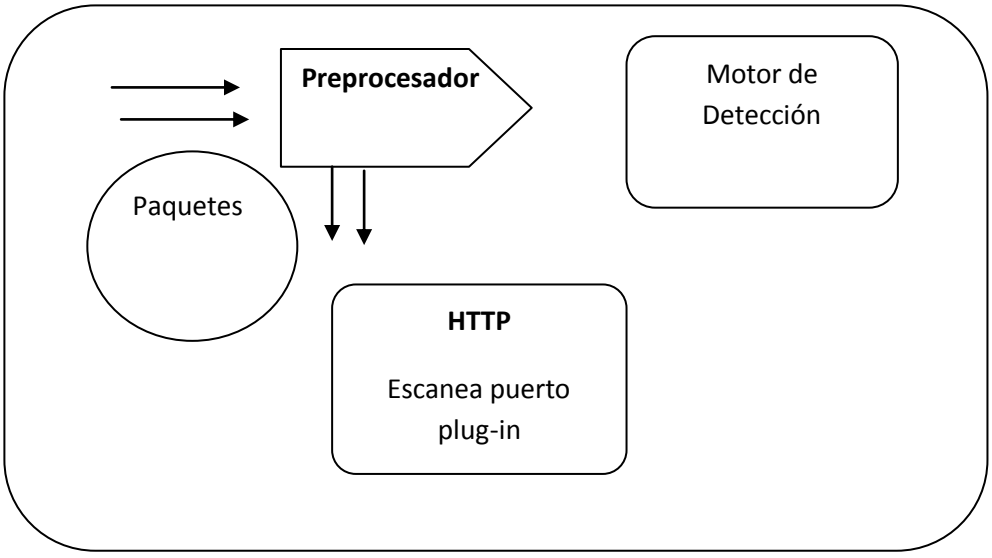


Imagen n°11: Autoría propia, Preprocesador

El preprocesador, actúa de manera, recibiendo todos los paquetes de data en la red, el cual utiliza un plug. In, para escanear y verificar, y trasladar al motor de detección.

4.5.5 Motor de detección

El motor de detección es el más importante dentro de los procesos de detección IPS, desde el punto de vista de sistema de detección de intrusos. A partir de la información que pasa por el preprocesador y sus plug-ins determinados, el motor de detección, establece a partir del conjunto de reglas o personalizaciones Snort.

Este grupo de reglas están agrupados por ciertas categorías (troyanos, buffer overflows, ataques contra servicios web, entre otros medios de peligro.

Acciones motor de detección

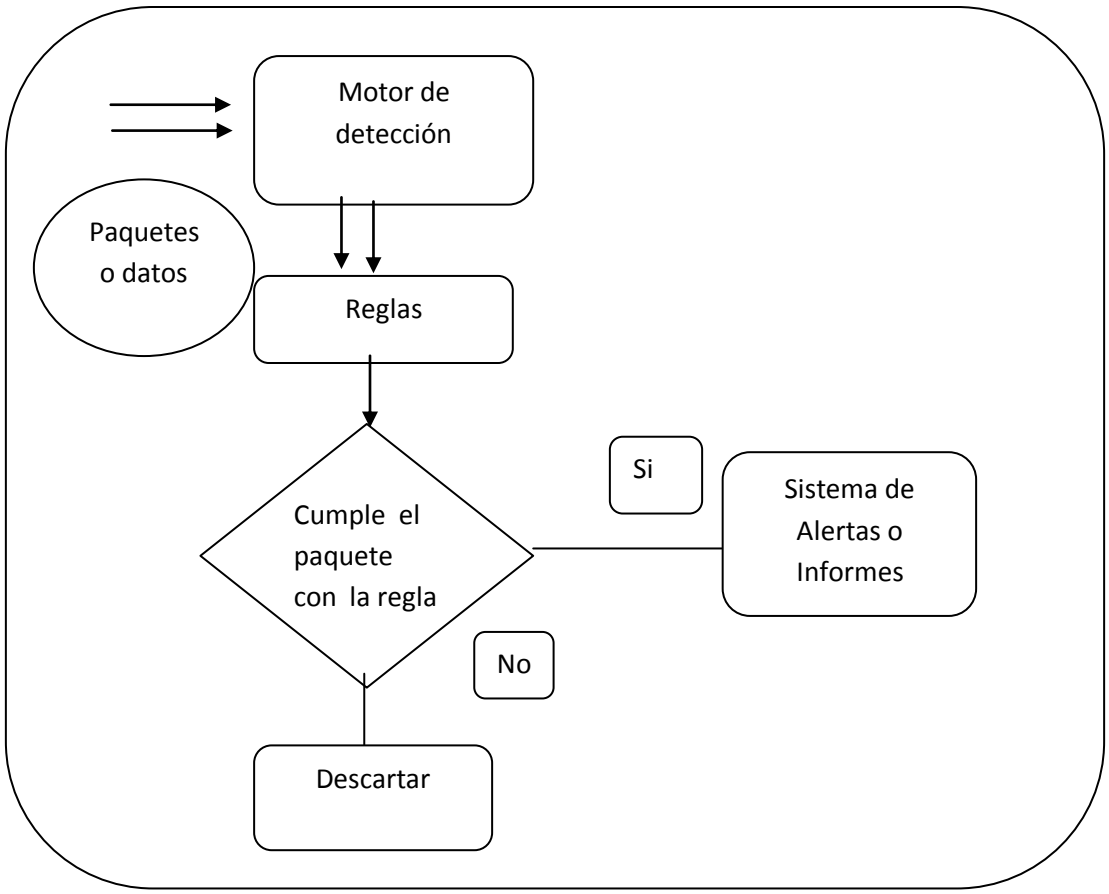


Imagen n°12: Autoría propia, Acciones motor de detección

4.5.6 Sistema de alertas e informes

Una vez que el grupo de paquetes o información, es atrapado por el decodificador de paquetes Snort, este medio de procesamiento, analiza por el motor de detección. Los resultados deben ser obtenidos de forma en que el administrador de la red, debe establecer de acuerdo a la necesidad de la política de la empresa.

Acciones de alertas e informes

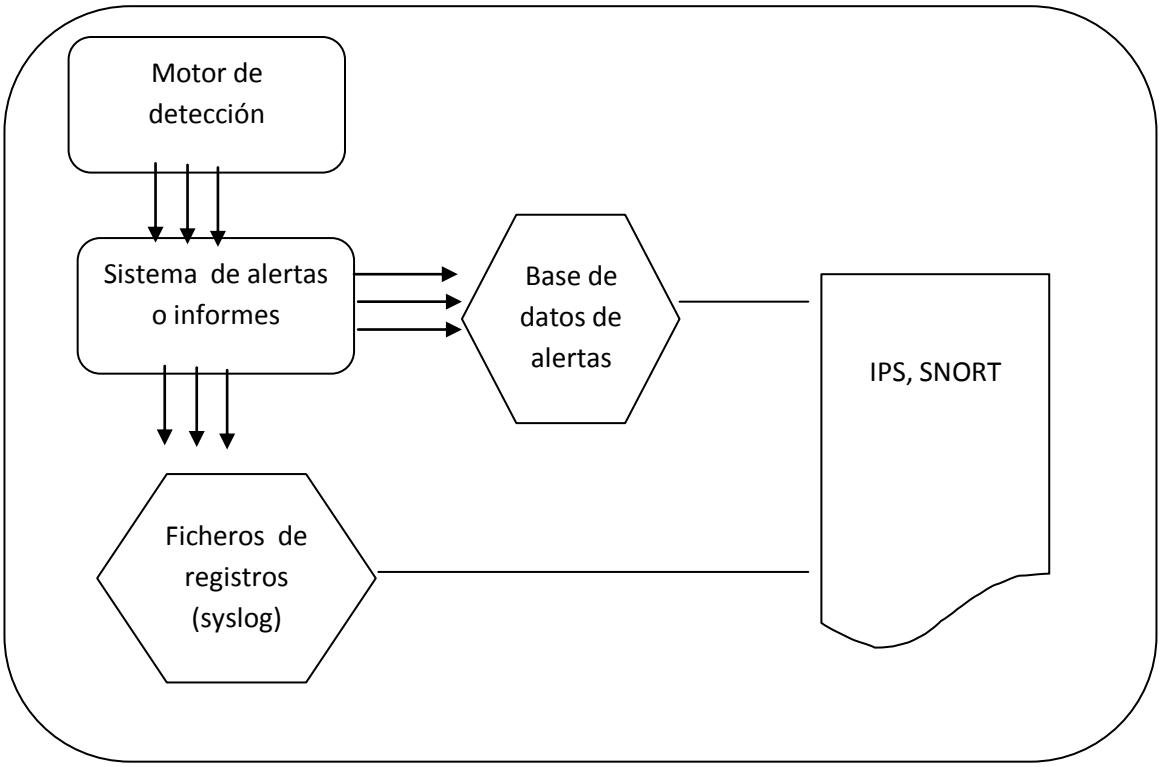


Imagen n°13: Autoría propia, Acciones de alertas e informes

Por último, destaca, que los Sistemas de Seguridad, basado en los Snort, conlleva la buena práctica de organización y control de seguridad evolutiva de alta disponibilidad incorporando mecanismos de acciones preventiva y correctiva para la empresa, para acciones de prevenir las vulnerabilidades de los diferentes procesos, mediante la arquitectura Snort.

4.6 (4).- Control y Protección de los datos por medio de un Antivirus y Anti spam (métodos inteligentes) Centralizados. [20]

ETAPA 4 (Anexo 3.1)

- Mantener la información segura durante la entrada y salida de datos a los llamados spyware, hackers.
- Control total de los servidores de la empresa

Generalidades

Cada una de las áreas de la Empresa Frada Sport, maneja una cantidad de información determinada, cada quien cumple sus funciones, pero ante el uso excesivo de de memorias flash, del uso exclusivo del cd rom, de compartir información en la red, y más aun, cuando una elevada cantidad de personal de la empresa no conoce los riesgos en internet.

El firewall como tal, incorpora métodos o mecanismos inteligentes basados en:

1. Motor de Antivirus Centralizado
2. Entrenamiento Spam Centralizado

Esta parte es importante, porque conlleva la buena práctica de prevención, de manera que se identifica a continuación, como se maneja cada servicio inteligente, basado en un control seguro centralizado ante toda la red de la Empresa Frada Sport.

4.6.1 Servicios de integración clamav

La herramienta como tal, gestiona diferentes tipos de servicios destinados a:

- WEB
- FTP
- ENTRE OTROS

Cada acción, representa diferentes procesos que maneja el clamav, ya que permite escanear ficheros de acceso, cuando es ingresado por cada usuario, sin embargo, su mejor funcionalidad, establece chequeos de directorios cada determinado tiempo, según su configuración previamente definida.

[20] Control y protección de datos, antivirus, anti spam

4.6.2 Funcionalidad clamav[21]

Su principal funcionalidad clamav, es inspeccionar el correo en los servidores SMTP de plataformas que incorpore el sistema de seguridad, que escanea, maneja, y controla comandos de sistema de actualización automático.

Identifica diferentes acciones de funcionalidad, basado en:

- Escanear bajo demanda.
- Actualización automática.
- Planificación de escaneos.
- Integración con diferentes navegadores en la red.

Incorpora, más procedimiento, basado en:

- Escaneo de flujo de datos en la red
- Establece ficheros infectados en el directorio.
- Registra la actividad de los escaneos en logs vivos, de sistema de seguridad.
- Indica rutas y ficheros a no escanear (lista blanca), número simultáneo de escaneos y tamaño máximo de ficheros de log vivos a procesar previamente definido.

También soporta documentos PDF, RTF, HTML y de Microsoft Office, debido a su alta disponibilidad establecida mediante su control actualizaciones basado en Camav.

Prevención software.- De la misma manera, el clamav como tal, interactúa de forma global en la empresa, examinando todo el conjunto de paquetes, las cuales se identifican riesgosas o no, es importante la creación de modelos de prevención. Que identifica y apunto al control clamav que gestiona el sistema de seguridad Endian Firewall.

[21] Recuperado de: http://www.alcancelibre.org/staticpages/index.php/como-clamav-centos,Clamav

4.6.3 Clamav antivirus centralizado

El endian firewall, cuenta con un control centralizado de antivirus, denominado (Clamav Antivirus), constituye el motor antivirus de código abierto, diseñado para la detección de:

- Troyanos
- Virus
- Malware
- Otras amenazas maliciosas.

Básicamente, es de suma importancia contar con un control centralizado para la Empresa Frada Sport, ya que proporciona un proceso de alto rendimiento basado en escaneo, es decir, examina todo el flujo de la red de cada una de las maquinas de las áreas de la empresa, utilidades de línea de comandos para el análisis de archivos, entre otros.

4.6.4 Entrenamiento spam centralizado *(Anexo 3.2)*

El spam consume determinado espacio en memoria, de las cuentas de correo y puede saturarlo, además de ocupar ancho de banda por el tráfico que genera en la red global de la empresa.

Es por esta razón, que se produce una pérdida o degradación del servicio de correo electrónico orientados a:

- Información de correo que demora un tiempo excedido a su destinatario
- Pérdida del servicio de correo
- Lentitud en la conexión de la red global de internet
- Desperdicio de espacio en memoria física y lógica.

Es la razón por la que la empresa como tal, implementa el uso de la herramienta de seguridad, basado en filtros, contra el spam.

4.6.5 Filtros de rendimiento que ofrece técnicas spam. [22]

Listas negras. Aquellos que tenga algún tipo de vulnerabilidad que permita relacionar con el spam. La información que llega al servidor Efw, no se toma en cuenta.

Listas blancas. Listas de servidores de confianza definido. Incluye de manera manual y admite los correos que venga de los servidores de correo determinado.

Análisis de cabeceras. Realiza una búsqueda de datos no existentes o incorrectos en los procesos o mecanismos spam, incluye la comprobación de que existe la dirección del remitente correcto.

Filtrado por campos. Todos los clientes de correo electrónico, permite clasificar el correo según la dirección o el dominio del origen de envió de determinados datos, o por la aparición de ciertas palabras en el asunto o en el cuerpo del mensaje que se presenta inusual.

4.6.6 Iniciativas anti-spam.

Se aborda la principal limitación que se encuentra al identificar, la autenticación del remitente, se encuentra:

Bloqueo de remitentes

Es muy eficiente, ya que evita la carga de ancho de banda en la red global, para analizar el mensaje, sino que al saber de quién procede, la herramienta puede bloquearlo sin recibir dicho contenido.

Listas negras de direcciones Ip (blacklists):

Este conjunto de listas negras, establece como un medio de prevención, estableciendo una lista de direcciones IP originadoras de spam (EFW).

[22] Fuente Instituto nacional de tecnología de la comunicación, Recuperado https://www.inteco.es/Formacion/Amenazas/correo_basura/Metodos_antiSpam/

Analizadores de contenido

Este mecanismos hace referencia a sistemas que, interpreta el mensaje y conlleva a analizar el contenido de paquetes de datos en la red, para encontrar un mecanismo que permita definir si el mensaje es legítimo o no.

4.6.7 Generalidades

Lo único que se establece, es activar la opción y borrar los correos procesados que considere correo “basura” o spam, cabe mencionar, que por el número de registros que pasan a través de todos los procesos que genera la empresa Frada Sport, en importante que el control spam, examine y verifique todo este tipo de registros de datos.

Esto hace posible, proceder a contar las palabras que aparecen en una muestra de mensajes deseados y no deseados, para asignar una probabilidad en función de su frecuencia de manejo de datos.

Las que aparezcan más a menudo en mensajes no deseados, tiene una probabilidad alta de ser parte de información altamente spam en la empresa.

Los spammers, hace posible, la utilización de técnicas como la inclusión de imágenes o archivos, basados en archivos tipo .pdf, .zip, .xls entre otros, en lugar de texto para esquivar a determinados filtros.

Los filtros de alta disponibilidad, establece métodos para clasificar qué correos son considerados como spam y cuáles son válidos. Ninguna técnica de filtrado es 100% efectiva para sí misma, pero si ayuda a controlar y a evitar distintas maneras de mensajes spam en la red de datos.

4.7 (5).-Mejorar el Rendimiento de los Equipos y de la Red [23]

ETAPA 5 (Anexo 4.1)

Procesos de desarrollo

- Permitir o denegar el paso de acceso a internet, a los usuarios de la empresa según su área
- Mejorar el rendimiento de los equipos y de la red, mediante el acceso y no acceso a internet, a los usuarios de la empresa, según el área en que se desempeñan.
- Control y seguridad a la hora de realizar, compras por internet, mediante métodos inteligentes.
- Control organizativo a los usuarios de la empresa, basado en crear políticas de seguridad, mediante especificar el tamaño máximo para descargar y subir archivos.
- Crear reglas de acceso, mediante autenticación para cada usuario
- Ver a que paginas ingreso cada usuario (registros. proxy)

4.7.1 Generalidades

Cada sección o modulo que se acopla a las necesidades de la empresa Frada Sport, conlleva diferentes procesos de configuración, para llegar al presente entorno orientado a las políticas de seguridad basado en crear reglas, filtro, accesos, denegación, control organizativo, que se establece bajo un control interno que la empresa como tal que desea incorporar.

Si se hace referencia a las encuestas basadas en políticas de seguridad, gran parte del personal de la empresa, no posee políticas de seguridad, sin embargo gozan de acceso total a internet, esto conlleva la buena y la práctica del correcto uso de aplicaciones, del internet, de saber o identificar correctamente los riesgos que posee determinadas páginas de internet.

Y sobre destacar porqué medio, los sistemas informáticos basados en software y hardware pueden sufrir vulnerabilidades.

[23] Mejorar el Rendimiento de los Equipos y de la Red

4.7.2 Control del manejo de la información

Se establece y se segmenta los puntos de acceso a cada usuario de la empresa, dependiendo del área, de la necesidad del internet que posea, totalmente contrario a los usuarios que simplemente se restrinja de forma global el internet, otros que se establezca ciertas páginas de navegación a internet, otros usuarios que se restrinja la descarga de información.

Referente al no acceso a internet, establece la no necesidad para un usuario determinado, al contrario, si un empleado como tal, crea políticas de seguridad mediante el control del acceso total, tomando en cuenta que este usuario no necesita, lo que se reflejara en este caso, es que, no trabaje, no rinda adecuadamente, se dedique a hacer obligaciones que no le competen, entre otros.

Para efectuar el mejor rendimiento de los equipos informáticos y de la red, se establecen parámetros de accesos de configuración basados en:

- **Red:**

  1.- Configuración de Anfitrión o añadir equipos a la red

- **PROXY HTTP SERVER:** [24]

  1.- Acceso Proxy

  2.-Autenticacion

  3.- Contenido de Filtros

  4.- Política de Acceso

- **Registros** [25]

  1.-Visor de Logs Vivos a nivel de proxy

[24] Recuperado de http://luvicast.blogspot.com/2011/06/appliance-de-proxy.html
[25] Recuperado de https://translations.launchpad.net/efw/trunk/+pots/efw/es/+filter?person=strokemeister

De manera general, sin aplicar ninguna política de control de acceso segmentado a la red para los usuarios determinados, se inicia los parámetros de configuración previa, basados en:

4.7.3 Red:

1.- Acceso de Anfitrión o añadir equipos a la red

Se crea o se añade usuarios a los equipos informáticos, basados en:

- ✓ Direcciones IP
- ✓ Nombre de equipo
- ✓ Nombre de Usuario

Lo que se estructura, es añadir los 10 puntos o usuarios de la empresa Frada Sport como punto de partida.

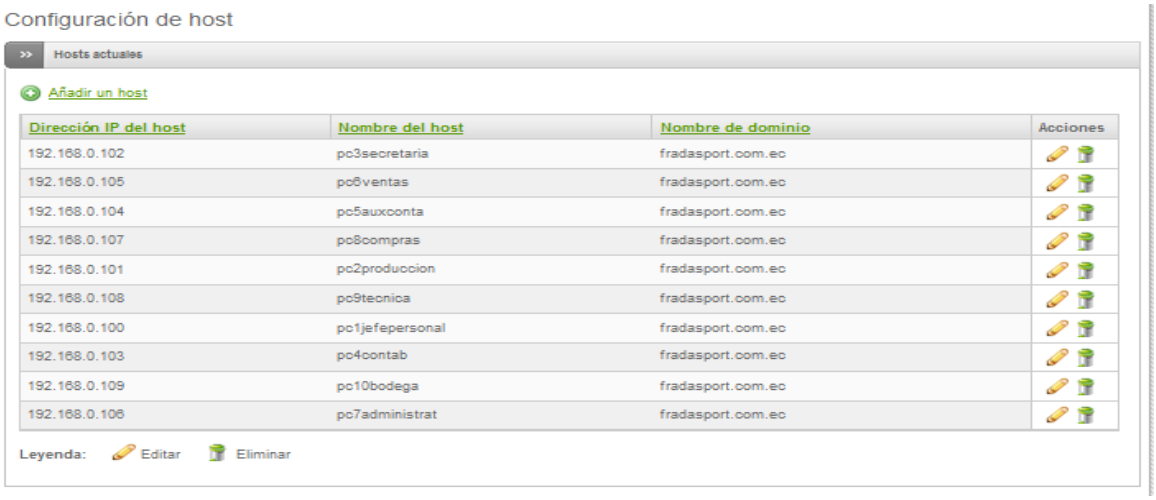


Imagen n°14: Autoría propia del sistema endian firewall, Añadir usuarios

Entonces, se incorporan todos los equipos de configuración de cada usuario de la empresa. Se parte desde la Ip 192.168.0.100 hasta la 192.168.0.109 que son los 10 equipos de la red para establecer políticas posteriores de acceso, así mismo en el nombre de equipo se identifica cada empleado con un número de pc, y el dominio basado en el nombre comercial de la empresa.

4.7.4 Segmentación de la red, aplicado a los usuarios de la empresa Frada Sport

ÁREAS A TRATAR IP	PC	ÁREA	POLÍTICA O CONTROL DE ACCESO/ NO ACCESO
192.168.0.100	Pc1	Área Compras	• Denegar acceso total a internet • Descarga de archivos • Autenticación • Restricción en descargas
192.168.0.101	Pc2	Área Producción	• Acceso a ciertas páginas de internet • Bloquear páginas de internet que no se será necesaria • Autenticación • Restricción en descargas •
192.168.0.102	Pc3	Área Secretaria	• Denegar acceso total a internet • Descarga de archivos • Autenticación • Restricción en descargas
192.168.0.103	Pc4	Área Contabilidad	• Acceso a ciertas páginas de internet • Bloquear páginas de internet que no se será necesaria • Autenticación • Restricción en descargas

192.168.0.104	Pc5	Área Auxiliar Contabilidad	• Acceso a ciertas páginas de internet • Bloquear páginas de internet que no se será necesaria • Autenticación • Restricción en descargas
192.168.0.105	Pc6	Área Ventas	• Denegar acceso total a internet • Descarga de archivos • Autenticación • Restricción en descargas
192.168.0.106	Pc7	Área Administrativa	• Acceso total a internet • Autenticación
192.168.0.107	Pc8	Área Jefe Personal	• Acceso total a internet • Autenticación
192.168.0.108	Pc9	Área Técnica y Tecnológica	• Denegar acceso total a internet • Descarga de archivos • Autenticación • Restricción en descargas
192.168.0.109	Pc10	Área Bodega	• Denegar acceso total a internet • Descarga de archivos • Autenticación • Restricción en descargas

4.7.5 PROXY HTTP SERVER:

1.- Acceso Proxy *(Anexo 4.2)*

- **Control organizativo a los usuarios de la empresa, basado en crear políticas de seguridad mediante especificar el tamaño máximo para descargar y subir archivos.**

Aplicado a las siguientes áreas de la Empresa:

Área Compras
Área Producción
Área Secretaria
Área Contabilidad
Área Auxiliar Contabilidad
Área Ventas
Área Técnica y Tecnológica
Área Bodega
Área Administrativa
Área Jefe Personal

Para realizar esta acción, se habilita el acceso que identifica que el proxy está en funcionamiento, en donde se establece las siguientes medidas:

Configuraciones de proxy:

- Parámetros de configuración:
- Puerto de acceso: 8080
- Nombre de equipos visible usando el proxy: Restricción
- Error en el idioma: Ingles
- Cuenta de correo usada para notificaciones: jacob_n20@hotmail.com
- Tamaño máxima de descarga KB: 0
- Tamaño máximo de subida KB: 0

Este procedimiento es el más importante en referencia a proxys no transparentes, mediante la restricción de subida y bajada de data.

Al ingresar el tamaño en 0Kb de descarga y subida de información, los usuario o empleados de la empresa de ciertas áreas mediante la segmentación, no podrán subir ni descargarse ningún medio de información como asunto de política de seguridad establecido en su área de trabajo.

Puertos permitidos:

Los puertos de control de accesibilidad, establecen accesos a las diferentes páginas web establecidas, si uno de los puertos no se establece en el grupo de acceso, simplemente no se accede a los diferentes medios de enlace definidos, los cuales son:

- Puerto 80 http
- Puerto 21 ftp
- Puerto 70 gopher
- Puerto 210 wais
- Puerto 280 http-mgmt

Acceso de registros

Las opciones que da por defecto y definidas por el sistema de seguridad, no establece ninguna actividad, cada uno de los registros habilitan o deshabilitan contenido accedido, sin embargo para las políticas, es necesario asignar cada registro que muestra, para crear puntos de registros, basados en:

- Habilitar registro
- Registro de filtro de contenido
- Registro de agente de usuario
- Firewall logging

Siempre debe de estar activado o habilitado el conjunto de registros, ya que conllevan procesos de contenido, conexiones salientes, políticas o denegación de accesos.

Estos son todos los requerimientos, que se debe de tomar en cuenta para la correcta administración de proxys http empleados, para los usuarios de la empresa Frada Sport.

2.-Autenticacion NCSA *(Anexo 4.3)*

- **4.7.6 Crear reglas de acceso, mediante autenticación para cada usuario**

Aplicado a las siguientes áreas de la Empresa:

Área Compras
Área Producción
Área Secretaria
Área Contabilidad
Área Auxiliar Contabilidad
Área Ventas
Área Administrativa
Área Jefe Personal
Área Técnica y Tecnológica
Área Bodega

El proceso de regla de acceso, mediante control de autenticación, es aplicado a todas las áreas dentro de la empresa, como medio de control de entrada de los datos como muestra de política de seguridad.

Es relativamente importante, debido a su simplicidad de accesos. Almacena los nombres de usuario y contraseñas en un archivo de texto, Este formato de archivo de contraseñas constituye control de registros HTTP NCSA.

Acceso especifico Ncsa a nivel de usuarios

El contenido de registros NCSA a nivel de usuario, constituye una parte fundamental para los usuarios de la empresa, en donde se ve reflejado cada empleado dependiendo del área de trabajo, todo el grupo de empleados, establece control organizativo de los datos, elevando un porcentaje elevado de seguridad funcional.

Asignación de usuario y contraseña a cada empleado:

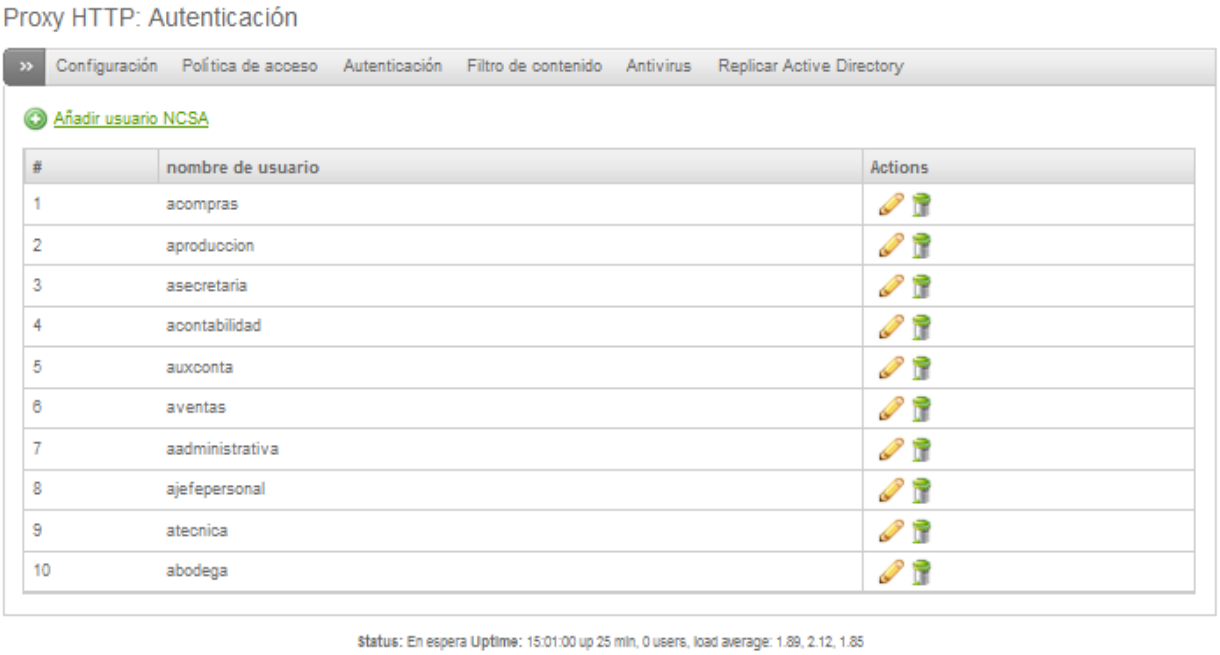


Imagen n°15: Autoría propia del sistema endian firewall, Usuarios autenticación

Cada empleado de la empresa, posee un medio de seguridad, basado en establecer autenticación, por medio de un usuario y contraseña determinada en la red global de datos.

3.- **Contenido de Filtros** *(Anexo 4.4)*

4.7.7 DENEGAR ACCESO TOTAL A INTERNET (Anexo 4.5)

Aplicado a las siguientes áreas de la Empresa:

Área Compras
Área Secretaria
Área Ventas
Área Técnica y Tecnológica
Área de Bodega

Perfil de Desarrollo

El control, perfil de filtros de contenidos, establece políticas de seguridad, orientadas en la empresa a, gestionar controles de accesos limitados a la web, es decir, este grupo de acciones y procesos, constituye el acceso no autorizado total a internet.

De acuerdo a la segmentación de la red global en la empresa, las áreas destinadas al *no acceso al sistema*, establece medios de seguridad que no se involucra con la necesidad del uso del internet de ciertas áreas de trabajo, basado en:

Bloquear Filtros de contenidos de listas de categorías como:

- Webs Adulto
- Webs Audio
- Webs Citas
- Webs Foros
- Webs Juegos
- Webs Noticias
- Viajes
- Webs Anuncios
- Webs Chat
- Webs Violencia
- Pornografía

Hace referencia, a todo el paquete de información que pasa en la red, es decir, según la segmentación dependiendo de las áreas de trabajo, no tiene acceso a internet.

4.7.1.1 ACCESO A CIERTO CONTENIDO DE INFORMACION *(Anexo 4.6)*

Aplicado a las siguientes áreas de la Empresa:

Área Contabilidad
Área Auxiliar Contabilidad
Área Producción

Maneja el mismo control de filtros de contenidos, pero en este caso, se define procesos de acceso a internet.

Este proceso, también maneja contenidos de los cuales, se limita a acceder, mediante contenidos de listas por categoría.

La diferencia está, en el cuadro de dialogo, que brinda el sistema se seguridad, agregar listas blancas o accesible para determinados usuarios de la red en la empresa, en donde se define la necesidad de determinados webs autorizados para ingresar.

Cuadro de dialogo de autorización:

Se define, páginas que es autorizado por el administrador de la red, estas páginas que maneja las áreas específicamente de contabilidad, tienen ingreso a webs como url de Bancos, del Sri, de seguro Social entre otras:

- sri.gob.ec
- pichincha.com
- coopjep.fin.ec
- servientrega.com.ec
- 29deoctubre.fin.ec
- bancodelaustro.com
- biess.fin.ec
- iess.gob.ec
- supercias.gob.ec
- evisos.ec/compra-venta/telas.htm

4.7.1.2 ACCESO TOTAL A CONTENIDO DE INFORMACION *(Anexo 4.7)*

Aplicado a las siguientes áreas de la Empresa:

Área Administrativa
Área Jefe Personal

Perfil de Desarrollo

Este conjunto de procesos, describe la eficiencia y la correcta administración de los sistemas de seguridad, cabe mencionar, que los mecanismos de perfil que se crean, se controlan y brindan el acceso total de las páginas o webs de internet.

Tales áreas de trabajo, segmentan el acceso de todas las páginas, webs, url. Es decir, tiene el acceso 100% a todo el manejo de la información en la red global de la empresa Frada Sport como tal.

Ninguna lista de contenidos, dirigida a categorías de diferentes medios de páginas de internet, como medios de control de acceso, será bloqueada ni ajustadas como políticas de seguridad.

Tales áreas de trabajo, como la administrativa y jefe de personal, manejan mecanismos únicos en toda la empresa, que se involucran con todo el acceso físico y lógico de medios de información, más aun cuando existe acceso a páginas de internet.

4.7.8. Política de Acceso *(Anexo 4.8)*

Los controles que maneja el EFW, permite agregar funciones de acceso, de acuerdo a las políticas de seguridad dependiendo de área de trabajo.

4.8.1.1 Cuadro de ejecución de políticas

Filtro de Perfil	Usuarios Permitidos	Política
a administrativa	Acceso total	Filtro usado 1
A jefepersonal	Acceso total	Filtro usado 1

Filtro de Perfil	Usuarios Permitidos	Política
a compras	Acceso total denegado	Filtro usado 2
a secretaria	Acceso total denegado	Filtro usado 2
a ventas	Acceso total denegado	Filtro usado 2
a técnica	Acceso total denegado	Filtro usado 2
a bodega	Acceso total denegado	Filtro usado 2

Filtro de Perfil	Usuarios Permitidos	Política
a producción	Acceso a cierto contenido	Filtro usado 5
acontabilidad	Acceso a cierto contenido	Filtro usado 5
auxconta	Acceso a cierto contenido	Filtro usado 5

Modo gráfico, ejecución de políticas

#	Política	Origen	Destino	Grupo de autor/-usuario	Cuando	Agente de usuario	Actions
1	filter using 'content6'	CUALQUIERA	CUALQUIERA	aadministrativa ajefepersonal	Siempre	CUALQUIERA	
2	filter using 'content4'	CUALQUIERA	CUALQUIERA	acompras asecretaria aventas atecnica abodega	Siempre	CUALQUIERA	
3	filter using 'content5'	CUALQUIERA	CUALQUIERA	aproduccion acontabilidad auxconta	Siempre	CUALQUIERA	
4	filter using 'content1'	CUALQUIERA	CUALQUIERA	conta	Siempre	CUALQUIERA	
5	filter using 'content2'	CUALQUIERA	CUALQUIERA	no necesario	Siempre	CUALQUIERA	

Imagen n°16: Autoría propia del sistema endian firewall, ejecución de políticas

Control de vistas de url por usuario

Registros

A nivel de registros del EFW, constituye una parte fundamental para el control, organización y administración correcta de los usuarios de la empresa Frada Sport.

Cada usuario registrado con una Ip fija en la red global, permite que mencionada herramienta de seguridad, pueda obtener y guardar el historial de acceso a internet, es decir, las áreas de la empresa, las cuales se dio acceso total a internet, permite saber, si el jefe de personal o el área administrativa, a que contenido de información accede.

Se toma como ejemplo, el usuario jefe de personal.

192.168.0.100	pc1jefepersonal	fradasport.com.ec	

Imagen n°17: Autoría propia del sistema endian firewall, usuario jefe de personal

El usuario como tal, representa un empleado situado en un nivel jerárquico alto en la empresa Frada Sport.

Es por esta razón, que mencionado empleado, posee acceso total a internet, pero se toma como referencia, el historial de su acceso a internet, como asunto de control organizativo y administrativo que representa el sistema de seguridad, basado en registros proxy.

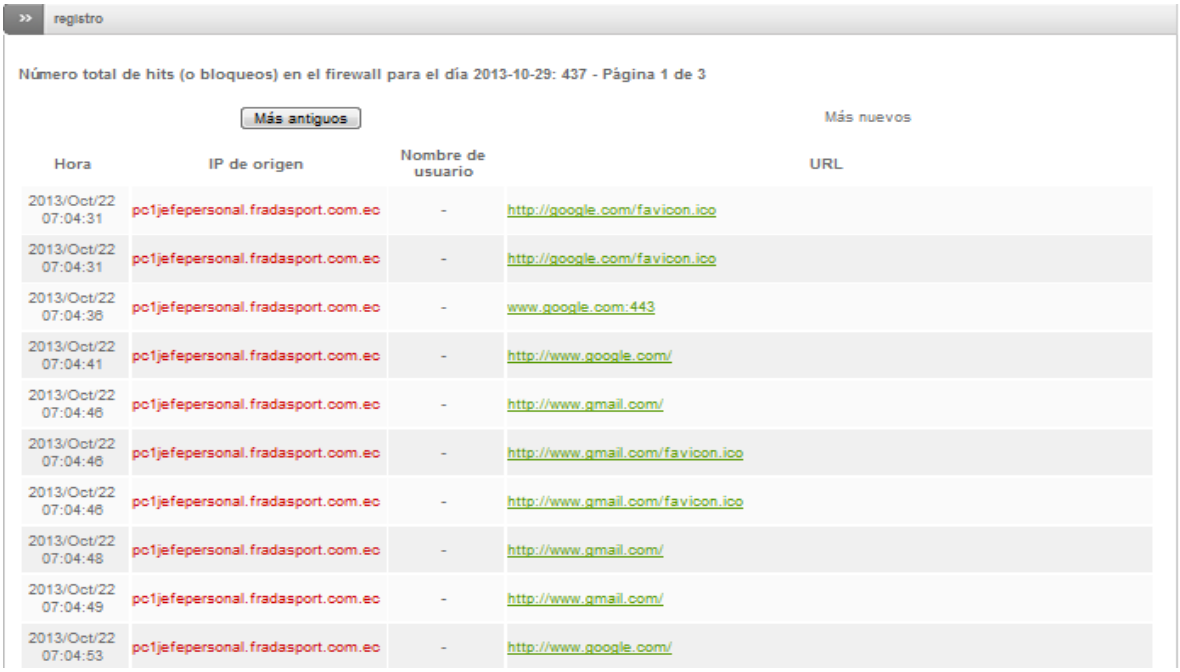


Imagen n°18: Autoría propia del sistema endian firewall, Registros Logs

Entonces, aparece, todo el contenido del usuario de acceso total, que se manifiesta como usuario: jefe de personal, más aun cuando existe un mejor rendimiento y registro para poder exportar a un archivo .txt. Todo el contenido de información, que el usuario accede en fechas determinadas, se encuentra registrado bajo un historial denominado *logs*.

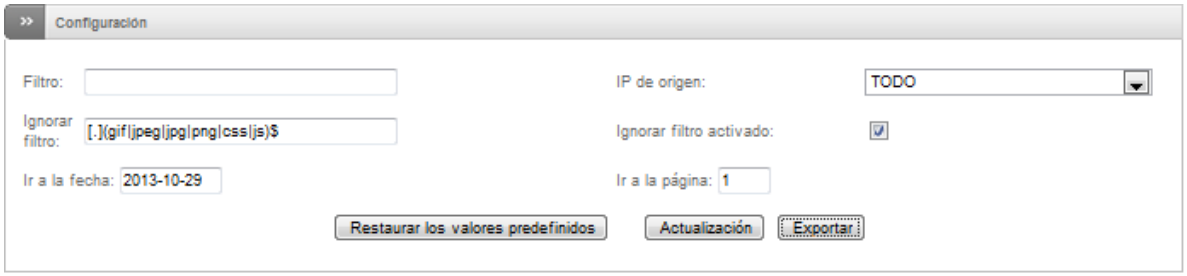


Imagen n°19: Autoría propia del sistema endian firewall, Exportar lista de Urls

4.8 (6).- Diagnosticar el Tráfico en la Red mediante el Sistema Endian firewall

ETAPA 6

4.8.1 Generalidades

Es importante realizar un análisis de cómo es el funcionamiento de la Ethernet en la empresa Frada Sport que posee acceso a la Lan.

Empezando diagnosticando, en base a las encuestas realizadas al personal de la empresa, se puede destacar que:

La mayoría de las personas que laboran en la empresa, poseen acceso a internet, por lo que da a conocer, que el personal en el trabajo, pueden acceder a cualquier método de información como: entretenimiento, páginas indebidas, redes sociales, etc. Decir también, que tales empleados, disponen de un acceso total y seguido, de páginas sociales como facebook, skype, Messenger, chat, entre otros.

Si bien se sabe que la gran mayoría de los empleados de la empresa tienen acceso a todo este medio de información basado en internet, es fácil establecer, que dicha empresa, no posee ningún medio o política de seguridad, que ayude a tener control y una organización a sus empleados para mejorar el comportamiento estructural y organizacional de la empresa.

Destacar también que, que al obtener acceso prácticamente, todos los empleados de la empresa, consumen e inestabiliza el flujo de la red, basada en el tráfico de la red, convirtiéndose lenta, caótica. En muchas circunstancias, el internet se pierde la comunicación de la red.

4.8.2 Consumo del ancho de banda de la red global[26]

El simplemente destacar, que mencionados empleados, tienen acceso a páginas de todo tipo cómo asunto de observación, las páginas que hoy en día se conoce, consumen gran cantidad de multimedia, es decir son webs dinámicas que incorporan publicidad, entrenamiento, juegos, chat, videos, música, etc.

---

[26] Análisis del Trafico, Recuperado https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD8QFjAB&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2F5j9r8LaoJvwuB2ZrJ-Xl7g&ei=AC2EUtKICoP64APw8oHACA&usg=AFQjCNE4oqIK3M17two8LxYZEC-VpEEeCw

Manifestar también que, estas páginas dinámicas, permite visualizar la información contenida en una base de datos, así como almacenar y hacer actualizaciones de cierta información a través de formularios donde el usuario introduce contenidos.

A lo diferente que es en años anteriores, que tales páginas de internet, únicamente contienen información basada en páginas estáticas, que no representaban gran cantidad de volumen de data subida en la web, es decir, el contenido que manejan estas páginas, hacen referencia a contenido único html.

Descrito el proceso de manejo, se puede establecer, que el internet que maneja la empresa, la cual la proporciona el ISP Telconet, es muy lenta, a pesar que los ISP, proporcionan un ancho de banda de 3Mb Corporativos Estables.

La herramienta de desarrollo, cuenta con un mecanismo para, examinar la información detallada y precisar del consumo de recursos de red global, y monitorear aquéllas conectadas a Internet, de esta forma lograr gestionar el creciente volumen de tráfico web en función de categorías de contenido de la empresa como tal.

4.8.3 Diagnosticar el tráfico entrante y saliente

Prever el volumen de tráfico de la red facilita controlar y manejar accesos provenientes de internet, la tendencia de utilización, se basa en crear políticas de seguridad.

El Firewall, representa una bitácora para diferentes funcionalidades, el punto principal, el tráfico de la red. En estado, representa diferentes modos gráficos para facilitar y estructurar de una manera correcta el tráfico en la red,

4.8.4 El servicio de análisis de tráfico de red le ofrece:

• **Descubrimiento y análisis de tráfico**. Establece y estructura el manejo de información que se encuentran corriendo sobre la red, y el uso de ancho de banda de tráfico entrante y saliente de la red global de la empresa.

• **Eficiencia en la red.** Incorpora determinado porcentaje de tráfico de la red global, apunta a la retransmisión de paquetes de datos, porción de tráfico y consumo de ancho de banda, estructurado a la cantidad uso de páginas webs de todos los usuarios de la empresa.

• **Utilización de ancho de banda.** Inspeccionar la utilización de procesos globales de datos en la red, para establecer la variabilidad en el uso de enlace y entender la capacidad del ancho de banda que maneja la red global.

4.8.5 Monitorizar la red global de la empresa

No se puede predecir con certeza exacta el tráfico de la red global en la empresa, la carga en la red está atada a grandes fluctuaciones, errores y diferentes problemas que puede darse en un momento determinado.

Con la ayuda de la herramienta de seguridad que gestiona el Firewall, permite monitorear la red, se puede estructurar y conocer una mejor visión de lo que está ocurriendo en la red, para así poder detectar los problemas más fácilmente, e incluso en ocasiones, antes de que ocurran. Para prevenir riesgos, vulnerabilidades, imprecisión o fallas en la red.

Para monitorear la red de la empresa, se debe hacer de una forma efectiva los siguientes procesos:

1. Localizar los usuarios de la empresa que están usando un mayor ancho de banda (segmentación de la red).
2. Suministrar reportes e información en tiempo real de cada interfaz de la red que maneja el sistema de seguridad.
3. Solucionar los diferentes problemas que surjan en la red (estadísticas del tráfico).

Si el plan o estructura principal, apunta a monitorear el tráfico de la red de la empresa como tal, posiblemente no se necesita más que las funciones o procesos que maneja el sistema de seguridad. Sin embargo, se debe realizar un análisis adecuado y conciso para encontrar la mejor solución de monitorear de la red global.

4.9 Test, Diseño del Emprendimiento Firewall que se Implementa

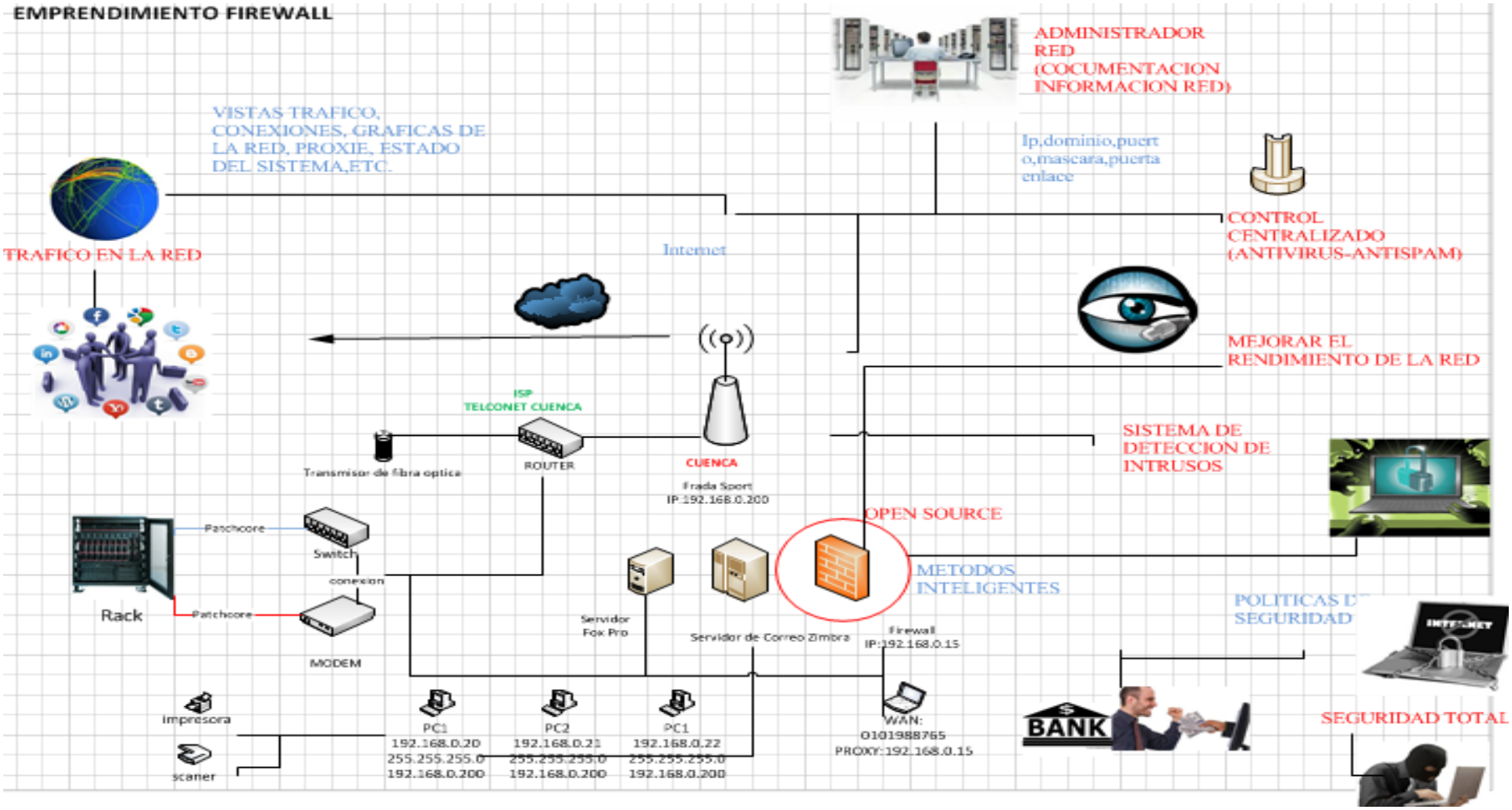


Imagen n°20: Autoría propia Microsoft Visio 2010, Diseño del Emprendimiento Firewall que se Implementa

4.10 Resultados de los Métodos inteligentes, basados en el Sistema Endian Firewall

TEMARIOS:

4.10.1 (1).- Test, Incorporar un sistema de Seguridad Open Source, abaratando Costos y medidas de prevención basado en mecanismos de seguridad.

- Sistema de Seguridad, abaratando costos

Referencia cruzada de la encuesta

- **Sistema de seguridad, abaratando costos**

4.10.2 Modelo actual de desarrollo

Los resultados esperados de la empresa Frada Sport, involucran procesos de bajo costos o que represente costos mínimos para la empresa.

Después de implementar y configurar el equipo principal, basado en el sistema de seguridad endian firewall.

El resultado ejemplifica un sistema de control y seguridad ya montado y en funcionamiento, es importante tener en cuenta que el sistema de seguridad EFW, establece políticas de seguridad, control y manejo de herramientas de alta disponibilidad.

El sistema como tal, protege la red global, de accesos no autorizados interna o externamente para aprovechar vulnerabilidades de los sistemas informáticos.

También destacar, que los usuarios de las cuales se crearan políticas o reglas de seguridad, se define en función a tales usuarios según las necesidades de su trabajo indispensable para cada departamento dentro de la empresa.

4.10.3 Beneficios

Uno de los beneficios claves y más destacados del firewall en Internet, es que simplifica los trabajos de administración, una vez consolida la seguridad en el sistema firewall, es mejor la distribución el control y la administración. Cada uno de los servidores que integran la red global de la empresa, en este caso los servidores fox pro y servidor de correo.

El firewall open source, ofrece un punto donde la seguridad puede ser:

- Monitoreada
- Controlada
- Gestionada
- Centralizada

Si aparece alguna actividad sospechosa, el sistema de seguridad, genera una alarma al administrador de la red ante la posibilidad de que ocurra un posible suceso inesperado como virus, detección de intrusos, smap, entre otros, basados en:

Imagen n°21: Autoría propia del sistema endian firewall, Servicios log

El sistema de seguridad, muestra diferentes medios gráficos, en donde llega la información en tiempo real, es decir, si habido ataques registrados, virus, correos rechazados entre otros. De esta manera, brinda un control total de registros entrantes y salientes de toda red de la empresa.

El sistema de alta disponibilidad y seguridad, destaca principalmente los bajos costos de implementación y accesibilidad.

Establece parámetros de acceso en donde se ve beneficiado la empresa de acuerdo a la necesidad de procesos de seguridad que gestiona el EFW.

Simplemente, con brindar un mecanismo de:

- Control
- Organización
- Política

Ofrece un punto, en donde reúne un mega sistema de bitácora, basado en la inspección y la prevención de intrusos no autorizados, que se pueda proteger o resguardar toda la información entrante y saliente de los diferentes procesos que hace que sea altamente importante y confidencial, según los medios de información de cada área en la empresa Frada Sport.

Los empleados de la empresa, ahora pueden acceder según el área en el labora, a ciertas webs de internet, otras no podrán hacerlo y otras áreas, tendrán el acceso total, de esta manera se reduce los riesgos al acceder al internet, al saber detectar medios o páginas inseguras, ya que el acceso es restringido, así como los daños en los equipos informáticos, el cual es reducido de una manera radical, y los costos operativos que maneja la empresa es totalmente menor.

4.10.4 Test, Configuración para inicializar el Endian Firewall

Para comprobar que el servidor Endian Firewall y una maquinan x de la empresa, se empieza comprobando la conectividad, en este caso:

1.- Se hace ping al servidor Endian Firewall para comprobar si los equipos se encuentran en red, en este caso, el servidor de seguridad, contiene la IP: 192.168.0.15 como puerta de enlace:

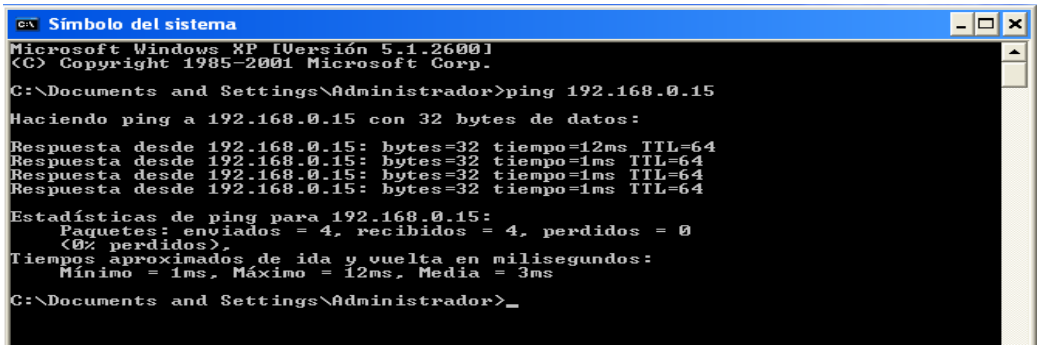


Imagen n°22: Autoría propia del sistema endian firewall, Ping al servidor

Después, se realiza, ping para comprobar si el servidor, se encuentra enlazado a los equipos informáticos de la empresa, en este caso, se toma la Ip, de una de las pcs de la empresa., en este caso:

Se ingresa a Shell, para poder hacer ping a la pc x de la empresa:

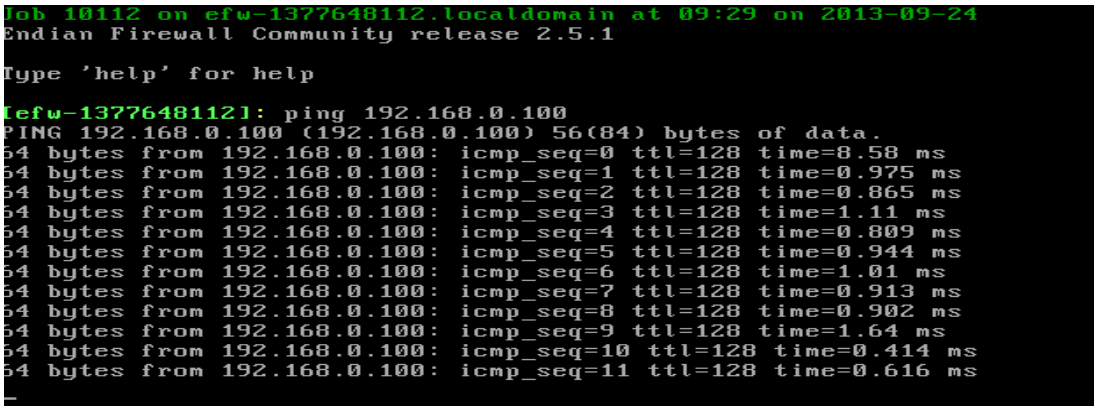


Imagen n°23: Autoría propia del sistema endian firewall, Ping a pc usuario

Las capturas en pantalla, demuestra que tanto, la máquina de la empresa, con el sistema de seguridad Endian Firewall, expone conectividad, para su correcto funcionamiento

4.11 (2).- Modelo de administración mediante, control y organización de los datos en la red, basados en subprocesos (sistema, estado, red y registros del endian firewall) de toda la información que pasa a través de la red.

- Documentar todo el sistema de manejo de las redes mediante el Endian Firewall que permita tener un nivel de control y organización para el administrador de la red.

Referencia cruzada de la encuesta

- **Documentar toda la información que pasa a través de la red, permitiendo un mayor control y organización de los datos en la red.**

Modelo actual de desarrollo

Los métodos que se centran en establecer procesos de control y organización de la red, identifica

4.11.1 Test, acceso a la red, establecido en los 10 pcs de la empresa

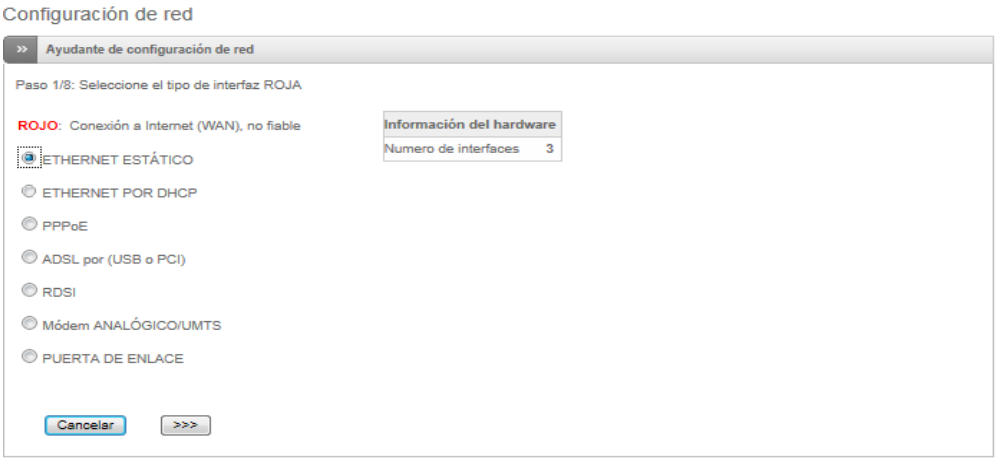


Imagen n°24: Autoría propia del sistema endian firewall, 10 pc usuarios.

4.11.2 Test, Notificación de Eventos

Imagen n°25: Autoría propia del sistema endian firewall, Notificación de Eventos

Es decir, virus, detecciones de intrusos, modo de cortafuegos, servicios habilitados o detenidos, entre oros, muestra, el sistema como tal, efectúa, envíos a registros de algún suceso del sistema al correo del administrador de la red.

4.11.3 Test, Web Console

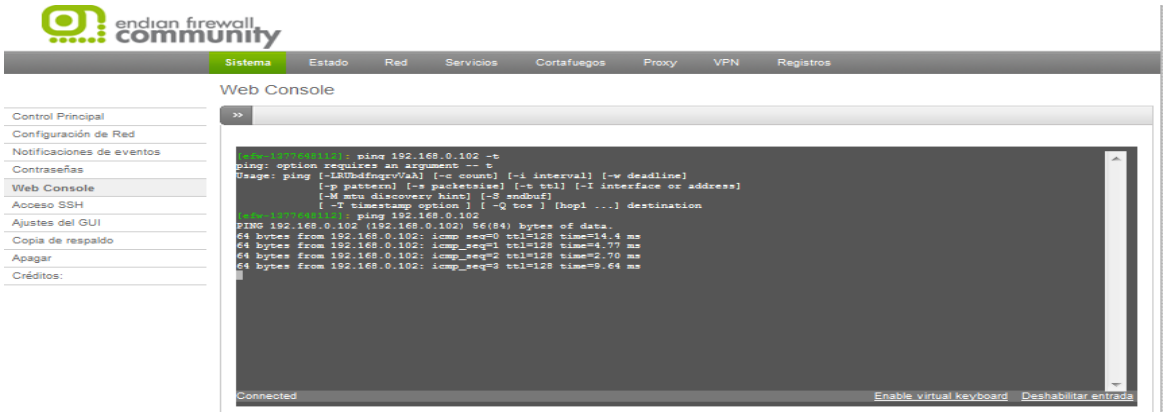


Imagen n°26: Autoría propia del sistema endian firewall, Web Console

Medio en donde se aplica acciones de control, basado en comprobar conectividad de los medios informáticos de la empresa, como se muestra en la imagen, se hace ping a una de las maquinas de la empresa, y esta efectúa la correcta conectividad. También para rutear, iniciar, restaurar los diferentes servicios que implementa el sistema de seguridad.

4.11.4 Estado del Sistema- Establece todos los servicios que gestiona el sistema de seguridad, en donde muestra todos los servicios activos e inactivos que mas hace referencia a la necesidad de la empresa.

Imagen n°27: Autoría propia del sistema endian firewall, Servicios on, off

4.11.5 Test, Conexiones:

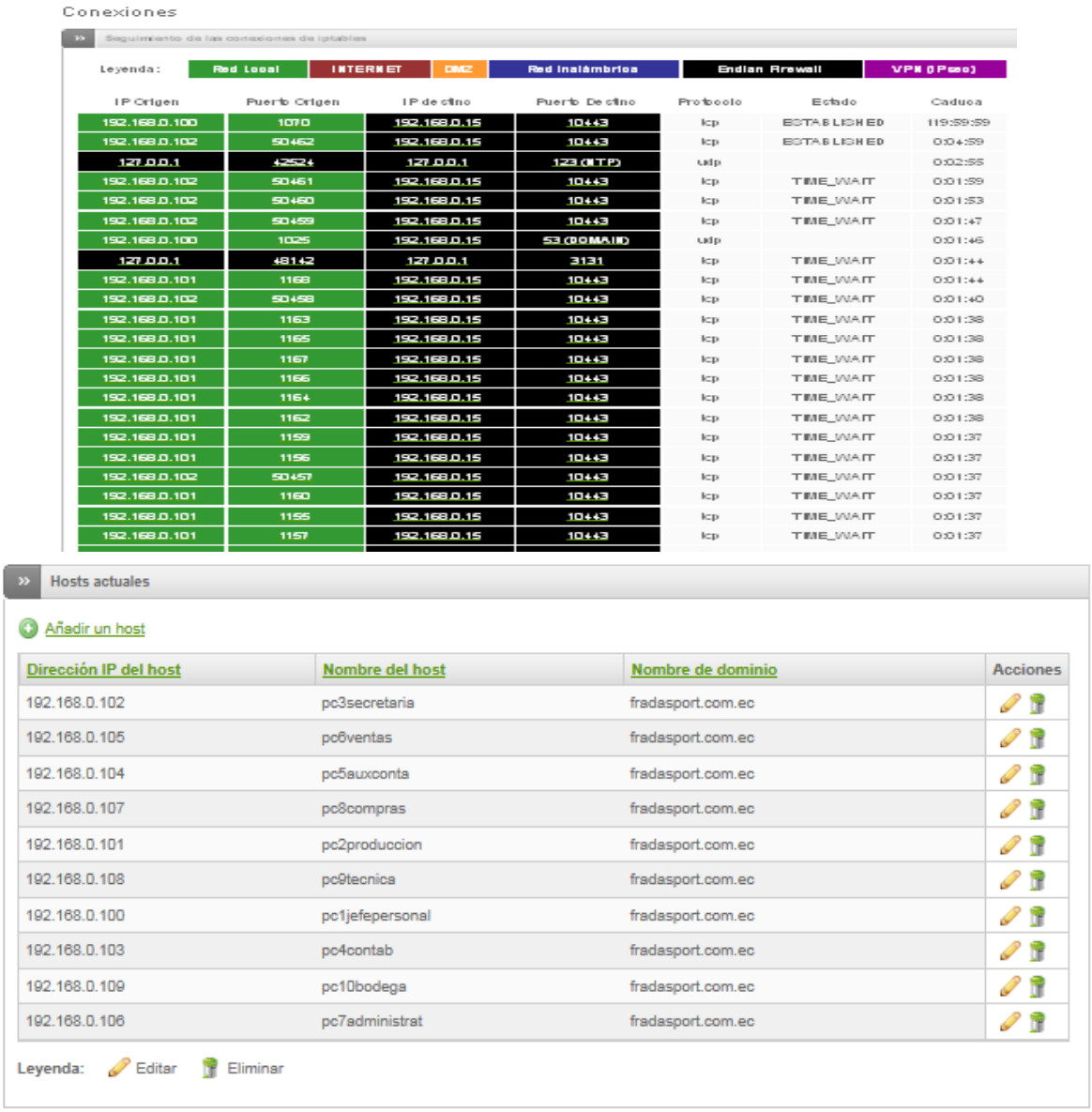


Imagen n°28: Autoría propia del sistema endian firewall, Conexiones

Ejecuta uno de los procesos más importantes, referentes a la correcta administración, y control de alto rendimiento en la red global de datos, también posee todo el flujo de administración de datos en la red automáticamente, para el administrador de la red en la empresa Frada Sport.

Se puede mencionar también, que es importante para la empresa y para el administrador de la red, contar con registros de datos de las maquinas, para conocer la Ip de máquina, los puertos que maneja, además si tienen o acceden a internet con los denominados Dmz, Y si poseen acceso a la red inalámbrica o ip fija, etc.

Es importante mencionar, que si por algún motivo, se requiere agregar más computadoras a la empresa, este registro de información, *ayuda a obtener datos certeros para poder crear algunas políticas, filtros, reglas, et*c.

Esto evita la duplicidad o redundancia de los datos, basado en: Ips, puertos, accesos, Entre otros, porque se vuelve en algunos momentos caóticos, por la inestabilidad de flujo de información.

Se tiene en cuenta y contando con esta herramienta de documentación de datos en la red, evita toda la pérdida de tiempo, en cuanto a duplicidad, errores de datos en la red, *además lo que conlleva la buena práctica de control administrativo de organización en la red y mejora el performance global de la empresa ,* además no existe falencias como daños en los equipos, al contrario, el sistema como tal, actúa como un sistema de brindar soporte a toda la red global, vigilando, examinando, estableciendo que sucesos a existido en in tiempo determinado.

Todo el conjunto de subprocesos o submenús que implementa el Endian Firewall, (*SISTEMA, ESTADO, RED Y REGISTROS),* genera que la empresa Frada Sport, esté al alcance de la tecnología, con herramientas únicas de control y organización en cuanta a manejo de procesos informáticos se refiere, la empresa como tal, ya no solamente maneja registros manuales, sino tecnología de punta, con sistemas inteligentes (Endian Firewall) únicos al alcance de todos.

4.12 (3).- Seguridad entrante y saliente de la información mediante un sistema de seguridad

- Mantener la información confidencial segura sobre todo los servidores con la incorporación de un sistema de seguridad.
- Control Automático, de auto detección de intrusos

Referencia cruzada de la encuesta

- **Permitir tener seguridad entrante y saliente de la información**
- **Mantener la información confidencial segura, sobre todo los servidores de la empresa.**

Modelo actual de desarrollo

Los ficheros de reglas Snort, implementa mecanismos de auto control, es decir, establece acciones en donde capta si algún elemento de toda la red global de la empresa, tiene registros sospechosos o maliciosos, en este caso, implementa herramientas de control como:

- Sitios indebidos,
- Maleware,
- Virus,
- Ataques a servidores web,
- Exploits,
- Conexiones p2p

Todo un compendio de reglas para proteger el entorno de agentes maliciosos y para limitar, obviamente, las libertades de los usuarios internos, sin embargo en próximas entradas se establece técnicas de evasión de IPS Firewall y otras “fortalezas” de los mecanismos de seguridad modernos como es el EFW de alta disponibilidad.

En la zona de registros del sistema de Seguridad, se muestra todos los componentes que procesan el IPS y el IDS.

4.12.1 Test, En donde se puede constatar que los resultados se vean reflejados en la ventana principal del servidor Endian Firewall, el cual muestra:

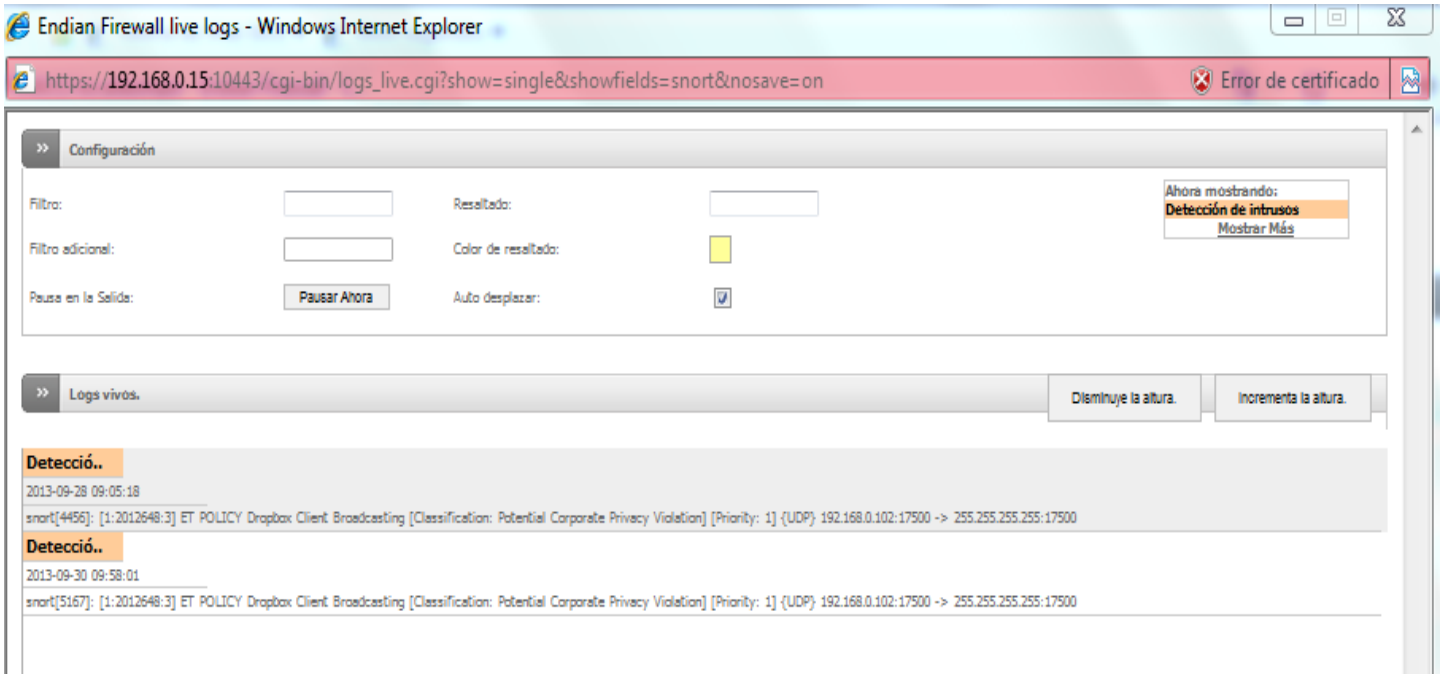


Imagen n°29: Autoría propia del sistema endian firewall, Detección potencial peligroso

Cabe mencionar, que anteriormente, la configuración realizada, basada en escaneo general en busca de programas, archivos, información, o inclusive detección de intrusos, se ve mostrada en la imagen principal.

Como se configura cada hora la agenda de actualización, este caso, se puede constatar que el Snort, encuentra contenido potencial elevado, basado en:

La imagen como tal, muestra en pantalla los denominados logs vivos, en este caso:

Muestra el año, mes y día, basados en las reglas Snort 4456 y 5167, en donde establece e indica un elevado potencial de contenido, en el que también, indica la Ip, que contiene mencionado contenido, en este caso 192.168.0.102, y por último, indica la hora, en las que se manifiesta, 9:05, y 9: 58.

4.12.2 Seguridad Servidores

Sin duda, las reglas SNORT, ofrece una alta disponibilidad que cuanto a seguridad se refiere, incorporando métodos inteligente de alta disponibilidad, basado en establecer políticas Snort, lo que conlleva la buena práctica de control y seguridad de los datos.

Es importante para la Empresa Frada Sport tener un sistema inteligente, basado en incorporar, la detección de intrusos, que puede ser internamente o externamente en el mal manejo de la información, en violentar sistemas o programas informáticos, o simplemente, la de querer externamente violentar los sistemas informáticos de la empresa.

También conocidos como IPS, los mecanismos o subsistemas inteligentes, cuentan con características altas, que protegen a los sistemas y procesos en cuanto al manejo de la información.

En la Empresa Frada Sport, los servidores propios, tales como, servidor de correo Zimbra y servidor Fox pro, ofrece en base a Snort, la posibilidad de manejar datos y procesos seguros, de modo que no se vean afectados bajo ningún esquema de riesgo o medios de vulnerabilidad.

Así determinadas áreas segmentadas en la empresa, ingresando a las urls o webs determinadas, el IPS, se encarga de examinar y actuar como un medio único de seguridad, es por esta razón que el sistema de Snort, se convierte en una política de seguridad alta y medida en la empresa Frada Sport.

4.13 (4).- Control y protección de los datos por medio de un antivirus y anti.spam (métodos inteligentes) centralizados.

- Mantener la información segura durante la entrada y salida de datos a los llamados spyware, hackers.
- Control total de los servidores de la empresa

Referencia cruzada de la encuesta

- **Control y protección de los datos por medio de un antivirus y anti-spam, métodos inteligentes.**

Modelo actual de desarrollo

Motor de antivirus clamav centralizado

Después de haber gestionado y configurado todos los procesos de control de antivirus, se comprueba de la siguiente manera.

En este caso, el área administrativa como tal, ingreso a ciertas páginas del cual, mencionada área, dentro de la empresa, posee acceso total de internet.

Esta persona o empleado del área, no sabe identificar los riesgos en internet, a pesar que cada computador de la empresa, posee un antivirus, de los cuales, en muchas áreas, no cuenta con un control estricto de la base de datos actualizados, entre otros.

El Motor de Antivirus, *Clamav,* cuenta con toda la base de datos para detectar a nivel general, no solamente a nivel de cada usuario o cada máquina de la empresa. Sino en lo que hace referencia a toda la red, detectar alguna anomalía.

Este empleado, ingresa a estas páginas de internet, redireccionandose por otros links, sin darse cuenta:

PÁGINAS WEB INFILTRADAS DE CONTENIDO MALICIOSO

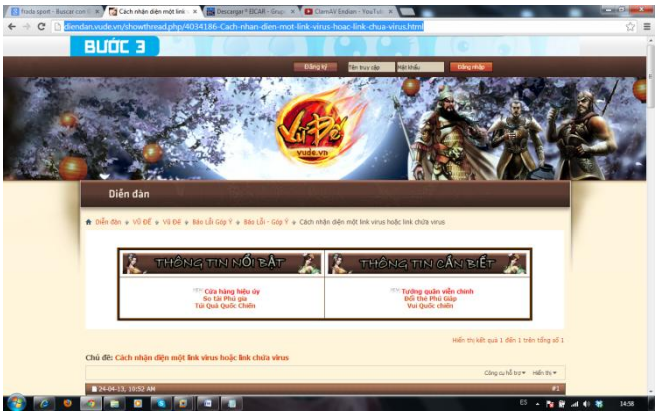


Imagen n°30[27], Url contenido de virus

Se tiene en cuenta, como actúa el motor centralizado del sistema de seguridad, este empleado sin saber a las páginas de internet que accede, y después de haber realizado todos los procesos de configuración para la detección de virus, se puede mencionar, que los niveles de seguridad y control para identificar riesgos, así, tales usuarios, no posean el conocimiento suficiente para identificar posibles virus, gusanos, troyanos, entre otros, es eficiente, para establecer altos.

De esta manera, queda establecido el acceso al sistema de internet, tomando en cuenta todas las acciones previamente realizadas en cuanto al motor de antivirus.

4.13.1 Test, *Entonces el resultado que incorpora el ClamAV es, sobre las páginas de internet, que el empleado de la empresa accede:*

[27] http://diendan.vude.vn/showthread.php/4034186-Cach-nhan-dien-mot-link-virus-hoac-link-chua-virus.html

Imagen n°31: Autoría propia del sistema endian firewall, Contenido Pishing

Establece mecanismos de control, basado en bloquear contenidos sospechosos, malicioso, basado en registros phishing, de la web de internet.

Test, el empleado de la empresa, también accede a otras páginas de internet, en donde establece:

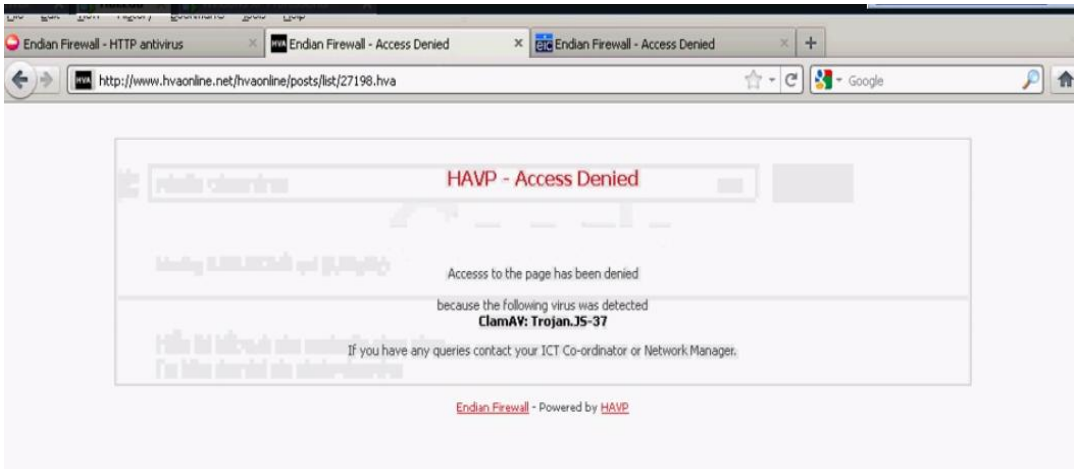


Imagen n°32 Autoría propia del sistema endian firewall, Contenido Tojan

Se puede manifestar, que el contenido que presenta la página de internet, posee contenido malicioso, basado en registros troyanos.

Creando todo el conjunto de configuraciones, que implementa el control de antivirus, se evita una gran cantidad de contenido malicioso. Muchos empleados, no se dan cuenta el manejo de información que presenta o manejan en la empresa, y sin embargo, contando con un antivirus, este programa apartado de la empresa no detecta nada.

Sin duda el contenido o subprograma que procesa el Endian Firewall, es de vital importancia, ya que brinda la posibilidad de proteger a la empresa interna y externamente de manejo seguro de información.

Decir también que si el motor de antivirus, si después de haber detectado páginas involucradas a contenido troyano, pishing, etc. Este se encarga de bloquear, impidiendo que se acceda a la página de internet, muy diferente a un programa cualquiera de antivirus, que si encuentra o detecta virus, se encarga de eliminarlo,

Diferente a lo que hace EL sistema de detección de virus, que se encarga de detectar amenazas y bloqueando el contenido, que resulta más rápido y flexible para toda el conjunto de interfaces o equipos en la red global de la empresa.

- **4.13.2 Anti spam Centralizado**

En registros se asigna, proxy Smtp:

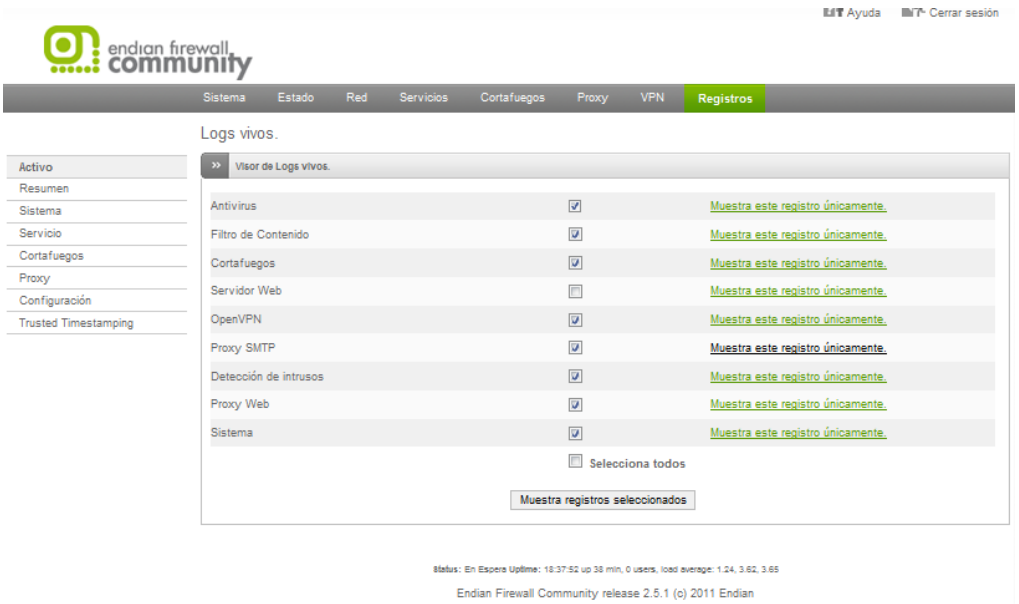


Imagen n°33: Autoría propia del sistema endian firewall, Registros SMTP

La herramienta de registros del sistema de seguridad, despliega un flujo o conjunto de información.

Si se verifica en la imagen, y después de haber configurado de ambas maneras el control inteligente basado en establecer el entrenamiento Spam Y Proxy SMTP, se puede establecer, que cada acción, bota un resultado determinante.

Los campos de entrenamiento spam, involucran procesos automáticos, por defecto que su función o característica principal es minimizar acciones de configuración, mas únicamente establecer aspectos básicos de la herramienta.

Sin embargo, existe otra manera no tan fácil de establecer configuraciones avanzadas de smap, y se basa en establecer por medio del proxy, lo que hace referencia al Smtp, en la zona de correo “basura”.

4.13.3 Test, Lo que se involucra en la sección, es manipular el mensaje spam de una forma correcta, basándose en establecer o agregar mensajes marcados como spam.

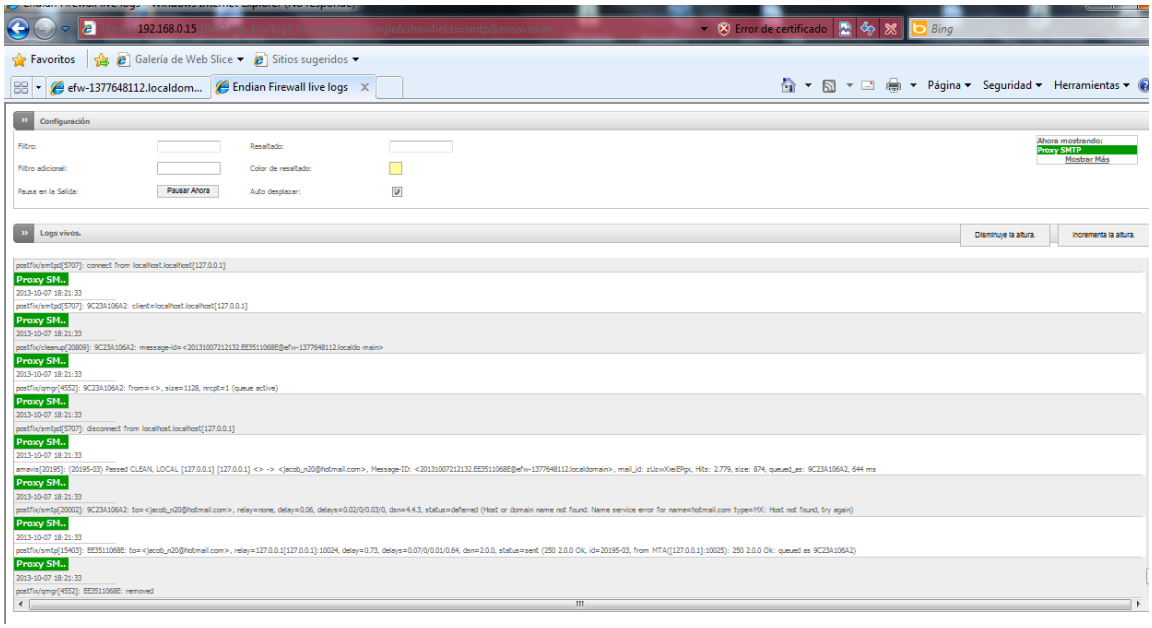


Imagen n°34: Autoría propia del sistema endian firewall, Logs Vivos SMTP

Se puede constatar en la imagen que muestra en pantalla, todos los mensajes de contenido spam, en este caso, de un usuario determinado en la empresa Frada Sport, cuyos mensajes o registros que captura el motor inteligente, basado en la búsqueda para mejorar el rendimiento de los equipos informáticos, establece lo siguiente:

- Primeramente se conecta al servidor, y capta el proxy transparente, basado en 127.0.0.1
- Identifica claramente al usuario cliente en el localhost, basado en el proxy
- Captura, y muestra en pantalla el mensaje lógico con un serial o registro único.
- Algunos registros, indica que este usuario se desconecta.
- Podemos también destacar, que este usuario que vuelve a conectar , y uno de los aspectos más importantes, establece el correo electrónico de la persona o usuario de la empresa que contiene registros o mensajes spam

Lo que da la posibilidad de contar con un sistema de ayuda, para identificar mensajes o contenido spam dentro de la red global de la empresa.

A pesar que los empleados de la empresa, dispongan de acceso al correo electrónico, las herramientas de alta disponibilidad, ayudan de una manera determinante y fiable a brindar seguridad física y lógica a la red de datos, identifican qué usuarios, mediante el correo electrónico manejan información “basura” o contenido spam, lo que destaca, que el administrador de la red, dispone de un medio de control para bloquear información “basura” para prevenir un mayor volumen de información no valida, no manejable de datos que consumen el ancho de banda de la red, y su performance.

4.14 (5.)-Mejorar el rendimiento de los equipos y de la red

Referencia cruzada de la encuesta

- **Mejorar el rendimiento de los equipos y de la red**
- **Políticas de seguridad**
- **Permitir o denegar el paso de acceso a internet, a los usuarios de la empresa según su área.**

Modelo actual de desarrollo

- **Proxy http server:**

1.- Acceso Proxy

- **Control organizativo a los usuarios de la empresa, basado en crear políticas de seguridad mediante especificar el tamaño máximo para descargar y subir archivos.**

PROXY HTTP

Imagen n°35: Autoría propia del sistema endian firewall, PROXY HTTP

Los usuarios segmentados en la red, al restringir el tamaño de descarga y subida en KB, dichos empleados no podrán subir ni descargarse información.

2.-Autenticacion NCSA

- **Crear reglas de acceso, mediante autenticación para cada usuario**

El proceso de regla de acceso, mediante control de autenticación, es aplicado a todas las áreas dentro de la empresa, como medio de control de entrada de los datos como muestra de política de seguridad.

4.14.1 Test, *Ejemplos de Autenticación.*

Empleado Compras

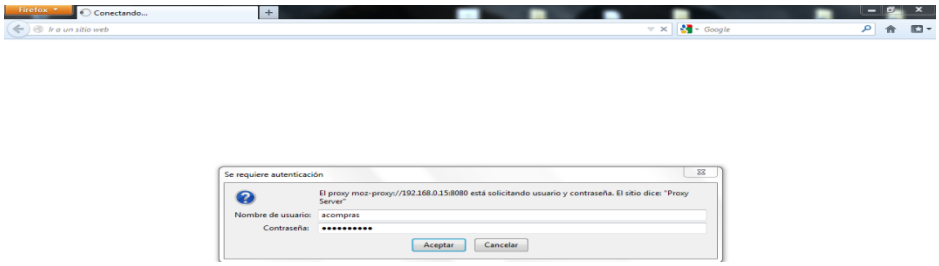


Imagen n°36 Autoría propia del sistema endian firewall, Autenticación

3.- Contenido de Filtros

DENEGAR ACCESO TOTAL A INTERNET

Perfil de Desarrollo

El control perfil de filtros de contenidos, establece políticas de seguridad, orientadas en la empresa a, gestionar controles de accesos limitados a la web, es decir, este grupo de acciones y procesos, constituye el acceso no autorizada total de internet.

Bloquear Filtros de contenidos de listas de categorías como:

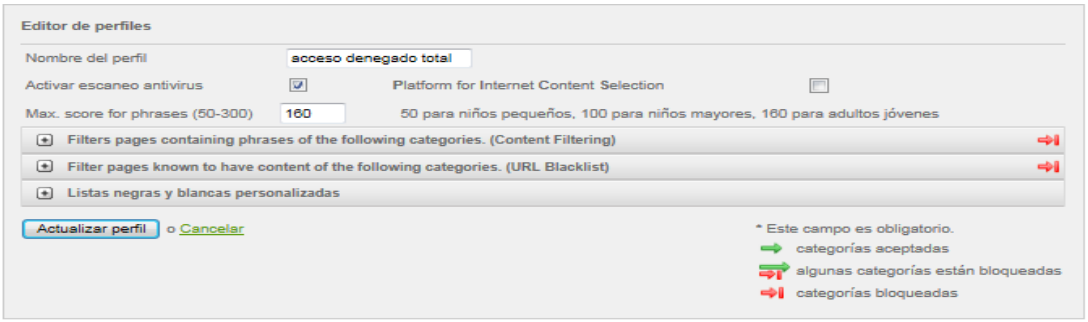


Imagen n°37 Autoría propia del sistema endian firewall, Bloquear Filtros

4.14.2 Test, *Resultado Saliente:*

Google.com

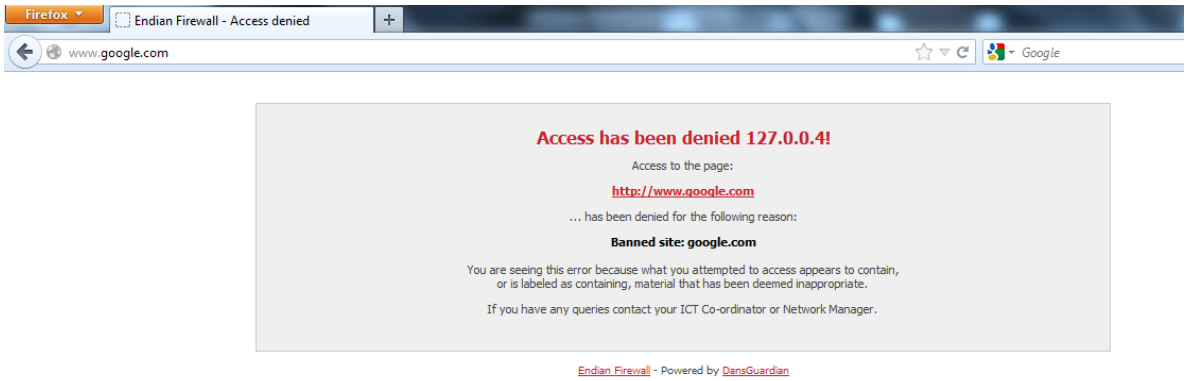


Imagen n°38 Autoría propia del sistema endian firewall, Resultado acceso

ACCESO A CIERTO CONTENIDO DE INFORMACION

La diferencia esta, en el cuadro de dialogo o listas negras o blancas, que brinda el sistema se seguridad, para determinados usuarios de la red en la empresa, en donde se define la necesidad de determinados webs autorizados para acceder.

Imagen n°39 Autoría propia del sistema endian firewall, Bloquear filtro Acceso a cierto contenido.

Listas negras y blancas personalizadas (acceso)

Imagen n°40 Autoría propia del sistema endian firewall, Listas personalizadas

Todo el contenido que hare referencia a, permitir los siguientes sitios, da el acceso de internet a los usuarios determinados de la empresa.

4.14.3 Test, *Resultado Saliente:*

Google.com

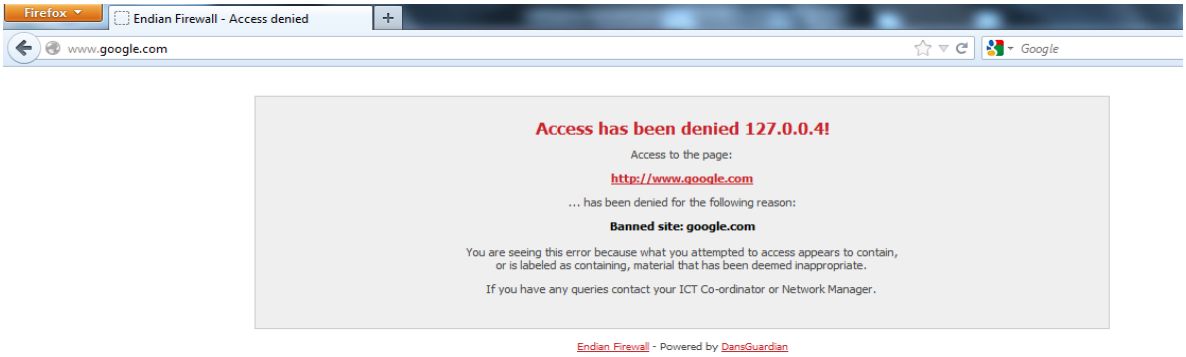


Imagen n°41 Autoría propia del sistema endian firewall, Resultado acceso

4.14.4 TEST, *CIERTO ACCESO DETERMINADO*

Contenido SRI

Imagen n°42[28], Resultado acceso determinado

[28] www.sri.gob.ec

En este proceso, el administrador de la red, deniega la mayor parte de contenido url, sin embargo, según la necesidad de ingreso, aprueba algunas páginas web.

ACCESO TOTAL A CONTENIDO DE INFORMACION

Tales áreas de trabajo, segmentan el acceso de todas las páginas, webs, url. Es decir, tiene el acceso 100% a todo el manejo de la información en la red global de la empresa Frada Sport como tal.

Ninguna lista de contenidos, dirigida a categorías de diferentes medios de páginas de internet, como medios de control de acceso, será bloqueada ni ajustadas como políticas de seguridad.

Estos filtros, involucran procesos de configuración predeterminada, es decir, no se bloquea, ni se registra procesos de acceso mediante:

Imagen n°43 Autoría propia del sistema endian firewall, Acceso Total

Generalidades

Los procesos aplicados mediante la segmentación de la red, corresponde a niveles de organización, control y la correcta administración de los usuarios de la red global de datos.

Lo que ejemplifica, que dichos empleados de la empresa, posean un nivel de restricciones en base a su necesidad de trabajo, lo que demuestra, que el grado de política de seguridad, es aplicable y funciona de una manera correcta en la empresa.

Así mismo, todos los usuarios de la empresa, poseen autenticación, para generar un medio de seguridad que permita posteriormente, dar acceso a determinado contenido.

Los usuario mediante la segmentación de la red de datos, establece el acceso total, así, no posean el conocimiento de identificar niveles de riego, el sistema de seguridad se encarga de manejar procesos únicos de control medido de seguridad, mediante el bloqueo de contenido malicioso.

Mencionados empleados, que poseen y manejan el computador en un nivel mayor a los otros, mediante la segmentación de la red, se determina que no poseen acceso a ningún medio de información web, es decir, corresponde a los usuarios que se restringe el acceso total.

De esta manera, los niveles de seguridad es mayor, por lo tanto, la empresa posee un nivel de sistema moderno, único y automatizado, capaz de resolver problemas y detectar a tiempo, es decir, el rendimiento de los equipos informáticos, se eleva en un nivel superior, previniendo posibles fallas, virus, mal manejo del computador, entre otros.

Lo que demuestra, en un alto nivel de seguridad, que el rendimiento de los equipos de software y hardware se mantiene en un nivel estable, eficiente, de alta disponibilidad y mejorada performance.

4.14.5 TEST, ACCESO TOTAL

Acceso a todo medio de información. Google.com, Hotmail.com, páginas de entretenimiento, redes sociales, chat, entre otros, es decir, todo acceso.

4.15 (6).- Diagnosticar el tráfico en la red mediante el sistema Endian firewall

- EL internet es muy lento debido a que múltiples usuarios tiene acceso a internet

Referencia cruzada de la encuesta

- **El internet es muy lento (tráfico en la red)**

Modelo actual de desarrollo

Beneficios del monitoreo del tráfico en la red

Si se monitoriza el tráfico de la red, se establece:

- Prevenir cuellos de botella de banda ancha empresarial, del rendimiento de servidores y equipos de las diferentes áreas de la empresa.
- Descubrir de acuerdo a un análisis en tiempo real, los días de más y menos tráfico en la red global de datos en la empresa.
- Actuar de forma proactiva y establecer un servicio estable ante el tráfico de red.
- Reducir el ancho de banda en la empresa de acuerdo a las áreas, mediante reglas de subida y descarga de archivos. (políticas de seguridad)

Gráficos de entrada, establecido mediante no congestionamiento de datos

Es simple darse cuenta, la herramienta como tal, implementa características muy inteligentes, dentro de estas, controlar de manera grafica en tráfico entrante y saliendo de la información de la empresa.

Se describe, indicando que el eth1 que corresponde al DMZ, es decir, las conexiones a internet que se enfocan claramente, y los br0 y eth0, relaciona, a los servidores propios de Fox Pro y Servidor de Correo, este mecanismo inteligente, actúa de forma global, es decir, capta todas las conexiones, mediante la configuración Tcp Ip o Ip fija. Se convierte en un sistema general que examina todo el paquete o flujo de información entrante y saliente de los procesos de la empresa Frada Sport.

Es representativo, dar énfasis a que en pocas ocasiones, es decir los días sábados y domingos, en la empresa Frada Sport, no posee un mayor tráfico en la red, debido a que los usuarios de la empresa no están laborando o cumpliendo sus actividades dentro de la misma.

Como el ejemplo a continuación.

Días Sábados y Domingos, Tráfico de las zonas entrantes y salientes.

4.15.1 Test, GRAFICOS ENTRADA

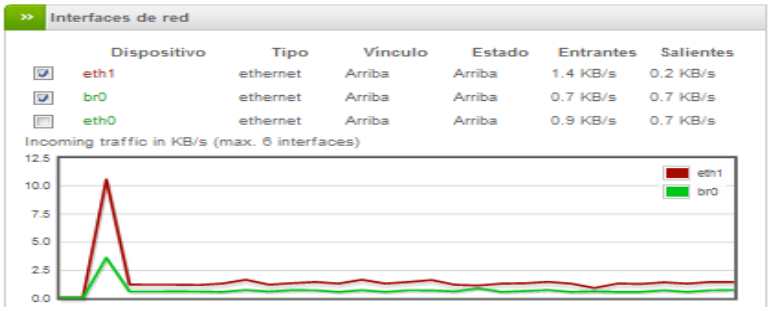


Imagen n°44: Autoría propia del sistema endian firewall, Grafico Entrada

Es importante destacar, que en los mencionados días, y como se puede diagnosticar en la imagen, la grafica, ejemplifica que las líneas de tiempo son visibles en un nivel bajo, es decir, las conexiones a internet son muy estables, con buenos puntos de acceso a internet, lo que da a conocer, que los ISP, o la conexión a internet es bastante buena.

4.15.2 Test, GRAFICOS SALIDA

Imagen n°45: Autoría propia del sistema endian firewall, Grafico Salida

Tráfico de entrada: paquetes de datos de red que entran al servidor (ejemplo: peticiones de descarga, peticiones de abrir tu página web, upload de archivos vía FTP, upload de archivos vía alguna aplicación web, etc.)De igual manera en este punto, las zonas o tráfico saliente, es bastante regular, esto hace referencia a paquetes de datos de red que salen del servidor red en cuestión (ejemplo: descarga de archivo de usuarios, descarga de imágenes y archivos solo por visitar tu página web, ver un video que tenga en el servidor, descarga de imágenes y archivos), como se puede observar, la línea de comando grafica esta en un nivel inferior.

Gráficos de entrada establecida mediante congestionamiento de datos

Días Lunes a Viernes, Tráfico de las zonas entrantes y salientes.

Si se toma referencia de las encuestas realizadas al personal de la empresa, en cuanto a la utilidad de internet, lo que manifiestan dichos empleados, es que el acceso a internet, es lento, consecuentemente, debido al acceso total de los usuarios al internet, es simple determinar, que los accesos originados de tales usuarios, correspondientes a *los días de lunes a viernes*, son bastante congestionados y caóticos, es por esta razón, el almacenamiento o páginas dinámicas que contienen ciertas páginas webs como:

- Redes Sociales
- Publicidad
- Entretenimiento

Estas páginas o algunas no mencionadas, contienen o almacenan gran cantidad de información en la cache, convirtiéndola en páginas totalmente dinámicas, por lo que establece un tráfico entrante y saliente de información muy elevado.

4.15.3 Test, GRAFICOS ENTRADA

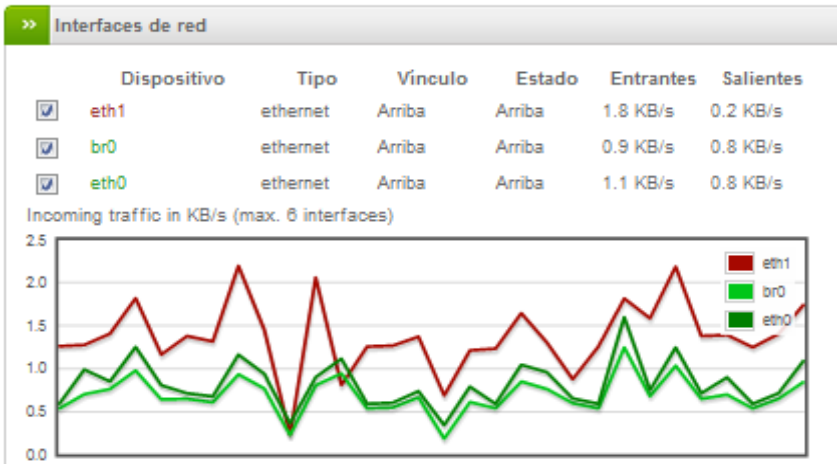


Imagen n°46: Autoría propia del sistema endian firewall, Grafico Entrada

Las líneas rojas, identifican, el acceso muy corrompido, lento, inestable de los diferentes accesos a internet, podemos destacar, que la inestabilidad del tráfico entrante, se encuentra por encima de lo normal, es decir, en un rango de 2.5.

4.15.4 Test, GRAFICOS SALIDA

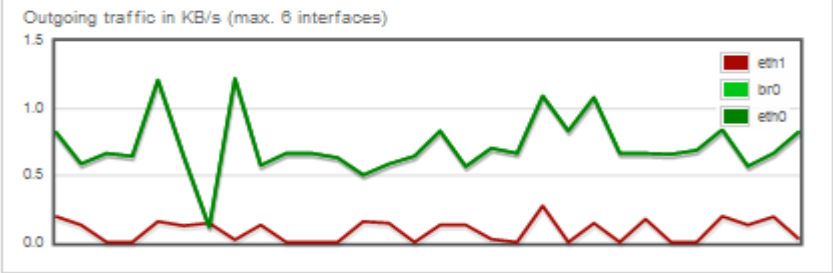


Imagen n°47: Autoría propia del sistema endian firewall, Grafico Salida

Las zonas o tráfico saliente, es bastante regular, las cuales se identifican con color verde, hace referencia a paquetes de datos de red que salen del servidor red, se encuentren muy inestables en cuestión (ejemplo: descarga de archivo de usuarios, descarga de imágenes y archivos solo por visitar páginas web, lo que marca en una zona de 1.5, en donde se encuentra un nivel muy alto.

Posteriormente, se identifica y se segmenta la red global de datos *(etapa 6*), dependiendo del área de trabajo, para efectuar posteriormente, políticas de seguridad, en donde el acceso es restringido, el nivel de descarga, entre otros, para generar por medio del tráfico en la red, niveles inferiores y estables ante las conexiones y acceso a internet, es decir, el acceso a internet, es limitado, ya no existe caídas de internet, posibles fallas de conectividad y acceso a la web.

Sistematización por medio de la segmentación de la red

Después de establecer la segmentación de los usuarios de la empresa, en base a políticas de seguridad, acceso y no acceso, los niveles de tráfico en la red, resuelven conectividad, tiempos de acceso, y lo más importante, líneas estables de comunicación, en base graficas que proporciona el sistema de seguridad Endian Firewall.

Es importante recalcar, que después de generar medios de seguridad en base a las necesidades de trabajo en la web para cada usuario, se reduce notablemente el tráfico en la red, es decir, las líneas se marcan y se mantienen en un nivel inferior, lo que demuestra, que el internet no se va, no se vuelve caótico, etc. Al contrario, se mantiene establece y fiable ante la conectividad de la red global de datos.

4.15.5 Test, *Ejemplificación ENTRADA, SALIDA.*

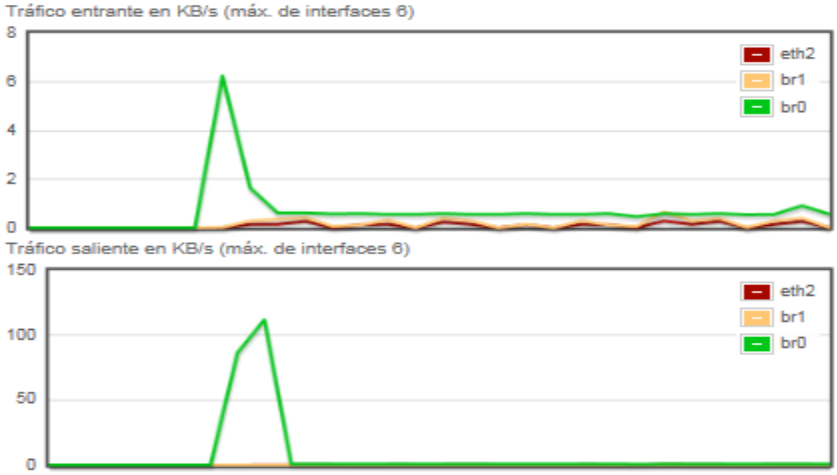


Imagen n°48: Autoría propia del sistema endian firewall, Segmentación Entrada, Salida

El tráfico entrante y saliente de la red global de datos, se regula en niveles inferiores, hasta cierto punto se eleva en un porcentaje de 6, en determinados acceso, que establece la segmentación de la red (*usuarios: jefe de personal, administración).*

Las denominadas, caídas de internet e inestable comunicación, se convierte ahora en una comunicación fiable, segura, sin tráfico y de alto rendimiento, tanto entrante como saliente y sobre todo, su alto rendimiento como mejor performance.

5. Conclusiones y Recomendaciones

5.1 Conclusiones

El sistema de seguridad Endian firewall, representa una manera estratégica de control, seguridad, disponibilidad, rendimiento y administración de la red global de datos, lo que se describe inicialmente, es un análisis de le empresa en técnicas de la investigación, basado en observación directa, encuestas descriptivas y referencia cruzada, para determinar el eje principal de la problemática de la empresa y abarcar procesos centrales de desarrollo.

Establecido el proceso de desarrollo en base a las encuestas, se analiza los diferentes medios de información vulnerables, puntos críticos, manejo de información de cada departamento de la empresa, entre otros, para representar gráficamente la situación actual referente a los diferentes problemas de la empresa como proceso de diseño.

Después, se procedió a estructurar la propia metodología de desarrollo, basada en 6 etapas de mejoramiento, cada etapa sigue diferente proceso de administración, control, seguridad, centralización y alta disponibilidad de datos.

Además, es importante trabajar con herramientas de entorno gráfico para tareas complejas, como crear reglas de filtrado, políticas, servicios, registros, entre otros.

Teniendo en cuenta todo el proceso a seguir, se puede manifestar que en la empresa Frada Sport, es aplicable el sistema de seguridad open source, basado en costos representativos mínimos para la empresa, toda la estructura física y lógica que gestiona el sistema de seguridad EFW, es de vital importancia, ya que cuenta con diferentes medios que ayuda a la empresa a tener principalmente seguridad centralizada de alta disponibilidad, y además, la correcta administración y control de todos los componentes de la red global de datos, destacando principalmente su alto rendimiento o performance .

5.2 Recomendaciones

- Realizar un correcto mantenimiento de la red global de datos, mediante el sistema de seguridad EFW.
- Chequear mensualmente los niveles de logs vivos, para identificar riesgos.
- Disponer constantemente, el uso de la herramienta de seguridad, para determinar y registrar nuevas conexiones e interfaces.
- Identificar posibles amenazas constantes, mediante los IPS, clamav centralizados.
- Identificar los niveles de tráfico, mediante la incorporación de más maquinas en la empresa.
- Tener siempre actualizado los motores centralizados, denominados clamav, spam, Ips, entre otros, para mayor seguridad y estabilidad.

Bibliografía

(2011). Arquitectura Snort. En J. G. Alfaro, *Deteccion de ataques en la red con Snort* (págs. 6-11).

ASI, A. d. (2010). *Poblacion y Muestra*. Obtenido de Poblacion y Muestra: http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/657.155%203-R696d/657.155%203-R696d-CAPITULO%20III.pdf

CETINA, Y. (7 de Mayo de 2012). *Seguridad en Redes*. Obtenido de Seguridad en Redes: http://www.slideshare.net/yesyduc10/conceptos-bsicos-de-seguridad-en-redes-11895594

Elit. (jueves de Junio de 2011). *Appliance de Proxy*. Obtenido de http://luvicast.blogspot.com/2011/06/appliance-de-proxy.html

Guerra, C. (2011). *Implementacion de una red segura.* Sangolquí.

Israel, U. (2013). *Plan estrategico.* quito: uisrael.

Juan, B. (2013). Análisis y Niveles de Riesgo, Observacion Directa.

Juan, B. (dic de 2013). Diseño y Análisis de la Situación Actual de la Empresa, ObDirecta. Cuenca.

Lazo, C. A. (2011). *Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas.* Quito.

Lykaios, E. (2011). Fundamentos Teoricos en Redes de Datos. *Fundamentos Teoricos en Redes de Datos* .

Macías, M. E. (2011). Administracion de la Red. En M. E. Macías, *Modelo Basico de la Administracion de la Red* (págs. 1-4).

María Fernanda Viteri Minaya, P. E. (2011). *"Metodología de Seguridad en Redes T.A.M.A.R.A: Testeo, Análisis y MAnejo de Redes y Accesos"* . Guayaquil Ecuador.

Merino, B. (Febrero de 2011). *Anáisis Trafico en la Red*. Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD8QFjAB&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2F5j9r8LaoJvwuB2ZrJ-Xl7g&ei=AC2EUtKICoP64APw8oHACA&usg=AFQjCNE4oqIK3M17two8LxYZEC-VpEEeCw

Moguel, E. A. (2010). *Metodología de la Investigación.* Mexico.

Ochoa, G. F. (Julio 2012). *Amenzas y Vulnerabilidades.* Sincelejo.

Onofre, E. J. (8 de julio de 2013). *Protocolo de Capa 7 Modelo Osi*. Obtenido de http://www.slideshare.net/eduardo_onofre123/protocolo-de-capa-7

Ponce, M. E. (Mayo de 2010). *Estadistica Inferencial*. Obtenido de Estadistica Inferencial: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.sisman.utm.edu.ec%2Flibros%2FFACULTAD%2520DE%2520CIENCIAS%2520ZOOT%25C3%2589CNICAS%2FCARRERA%2520DE%2520INGENIER%25C3%258DA%2520EN%2520INDUSTRIAS%2520AGR

Ramírez, I. H. (2010). *Modelo OSI*. Obtenido de Modelo OSI: http://www.institutomardecortes.edu.mx/apuntes/quinto/hprod2/unidadIII.pdf

Shram, D. (2010). *ClamAV en CentOS*. Obtenido de http://www.alcancelibre.org/staticpages/index.php/como-clamav-centos,Clamav

Xperts, M. (18 de Junio de 2012). *Modelo Tcp/Ip*. Obtenido de Modelo Tcp/Ip: http://mikrotikxperts.com/index.php/configuraciones/conocimientos-basicos/159-modelo-osi-y-tcp-ip

- Guillermo Fonseca Ochoa, Amenazas y vulnerabilidades, julio 2012
- Ma. Eugenia Macías Ríos, Modelo de Administración, 2011
- Recuperado: Fundamento en Redes http://tareastecisc.blogspot.com/2011/03/unidad-1-fundamentos-teoricos-de-redes.html
- Recuperado Modelo OSI: http://www.institutomardecortes.edu.mx/apuntes/quinto/hprod2/unidadIII.pdf
- Recuperado Modelo Tcp/Ip: http://mikrotikxperts.com/index.php/configuraciones/conocimientos-basicos/159-modelo-osi-y-tcp-ip
- Recuperado de: http://www.alcancelibre.org/staticpages/index.php/como-clamav-centos,Clamav
- Recuperado de http://luvicast.blogspot.com/2011/06/appliance-de-proxy.html
- Recuperado de https://translations.launchpad.net/efw/trunk/+pots/efw/es/+filter?person=strokemeister

- Análisis Tráfico, Recuperado:

  https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD8QFjAB&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2F5j9r8LaoJvwuB2ZrJ-Xl7g&ei=AC2EUtKICoP64APw8oHACA&usg=AFQjCNE4oqIK3M17two8LxYZEC-VpEEeCw

- Fuente Instituto nacional de tecnología de la comunicación, Recuperado de

  https://www.inteco.es/Formacion/Amenazas/correo_basura/Metodos_antiSpam/

Anexos

Manual de Procesos

INSTALACIÓN- CONFIGURACIÓN ENDIAN FIREWALL

(Ver Anexo 1.1)

Para empezar ya en la instalación del firewall, como punto de partida, se ejecuta y configura el sistema de seguridad y control Endian firewall, basado en la versión EFW-COMMUNITY-2.4.

Instalación del Endian Firewall

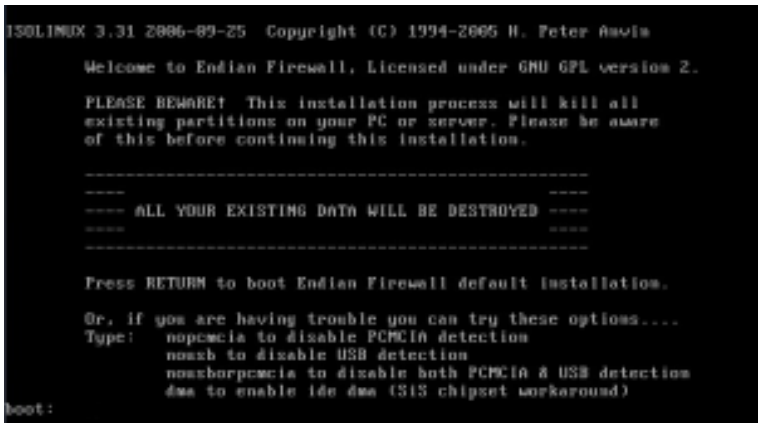


Imagen n°49: Instancian del EFW

En primer plano, en Endian Firewall, muestra la bienvenida de la instalación

Se Selecciona el idioma para continuar con la instalación.

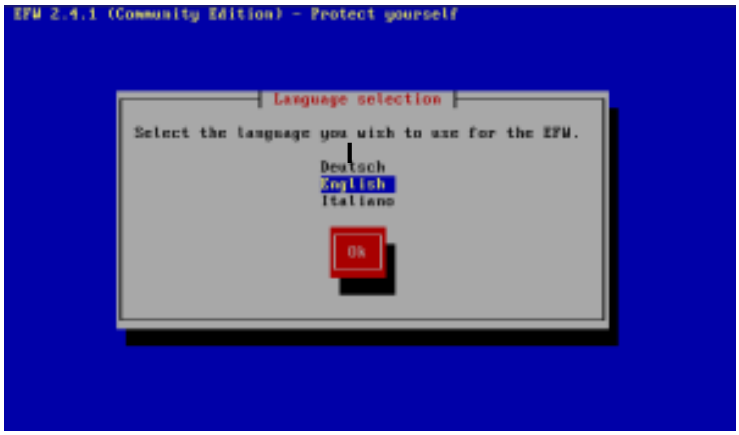


Imagen n°50: Instancian del EFW

Da la bienvenida de la instalación.

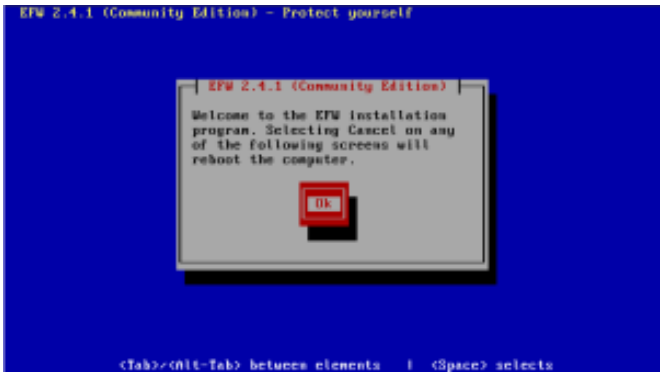


Imagen n°51: Instancian del EFW

Nos menciona si se desea particional los ficheros del sistema

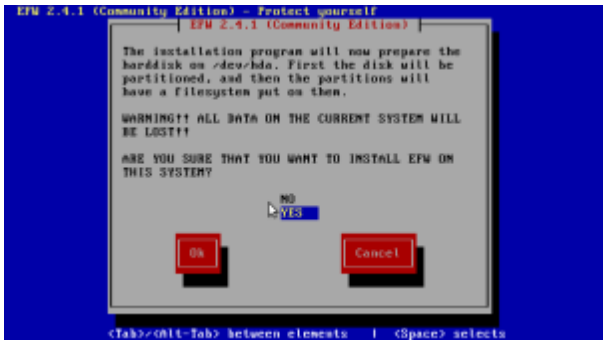


Imagen n°52: Instancian del EFW

Se selecciona ok para continuar.

Imagen n°53: Edición del EFW

Se habilita la consola del puerto serial

Imagen n°54: Habilitar puertos de Consola

Se espera, a que instale los paquetes necesarios y particiones el disco.

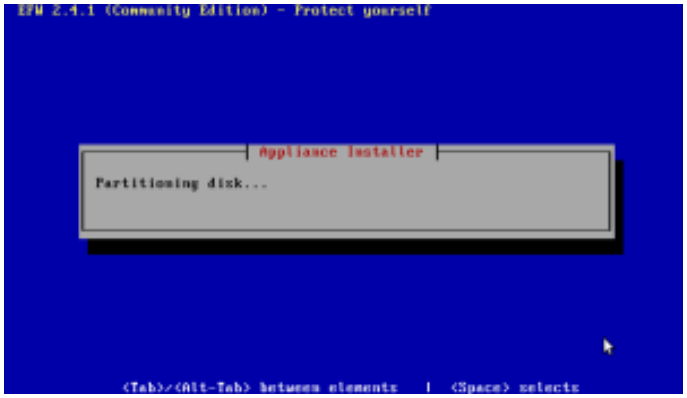


Imagen n°55: Particionado Disco

En esta parte, se coloca la dirección ip para la interfaz verde (LAN) o sea a la dirección de la red local del servidor endian firewall.

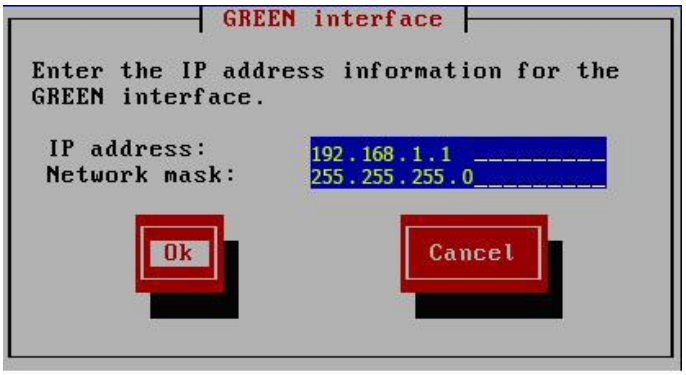


Imagen n°56: Asignación Ip de seguridad

Cada uno de los procesos de instalación, definen los procesos de consola, procesos de partición de disco duro, procesos de procesos de instalación de paquetes, de la IP

address que manejara el servidor, y la red de mascara, en donde el servidor propio de seguridad, se encontrara instalado correctamente.

Parte final de la instalacion:

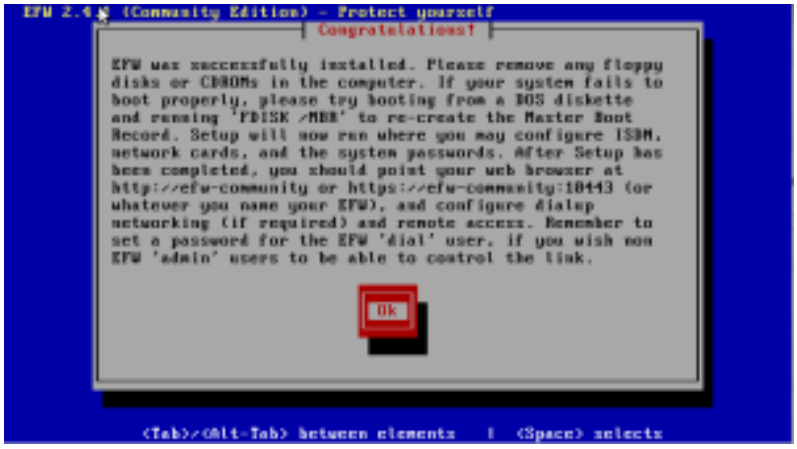


Imagen n°57: autoría propia del sistema endian firewall

Se reinicia la maquina y comienza a cargar todos los servicios que tiene por defecto.

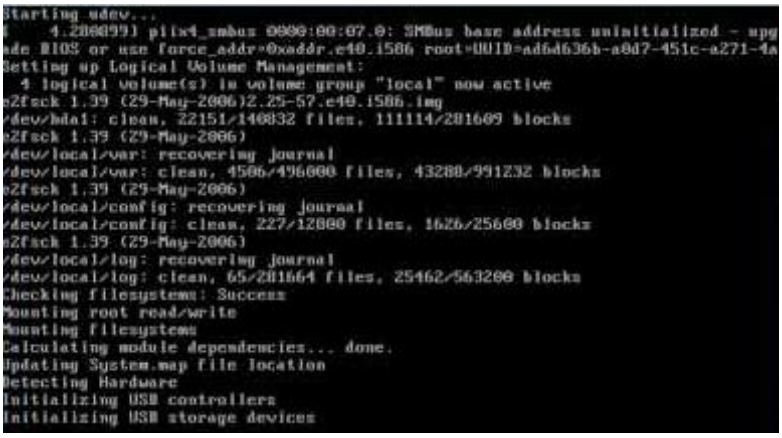


Imagen n°58: Reinicio de servicios y módulos a llamar

El servidor propio de seguridad, se basa en la IP: 192.168.0.15, representa la puerta de enlace en la que el servidor proporciona para los procesos o políticas de seguridad, en este caso:

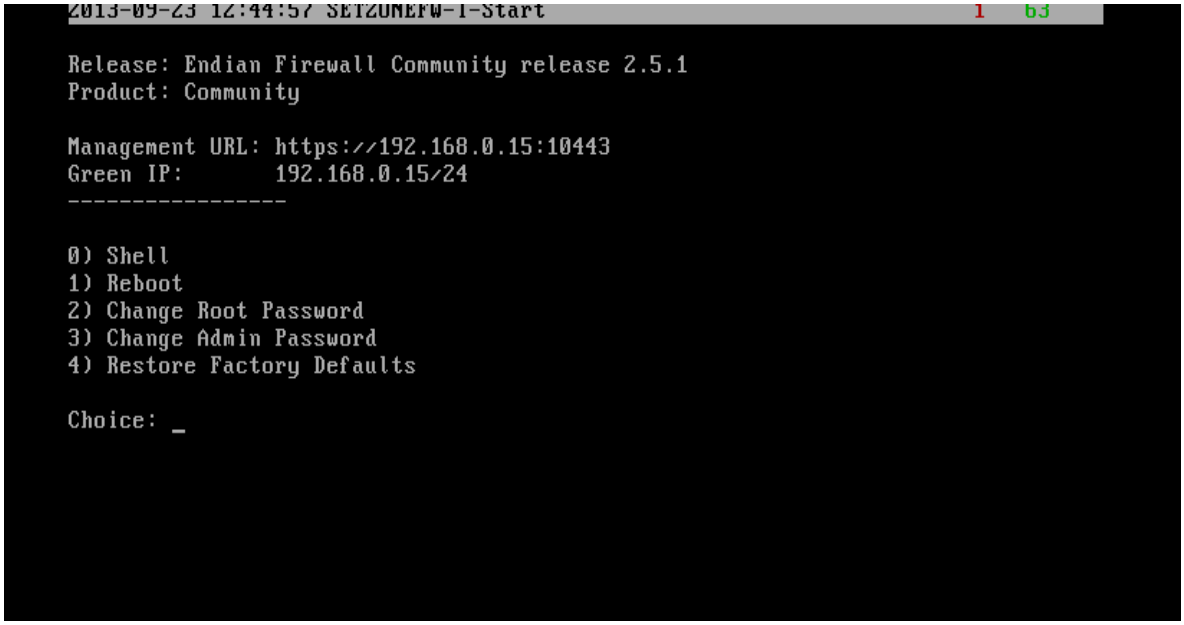


Imagen n°59: Carga de Modulos

Se procede a esperar unos minutos, hasta que todos los módulos o paquetes que contienen el sistema de seguridad se inicialicen de una manera correcta.

Ya establecido e inicialado lo módulos que contiene el Endian Firewall, se muestra en pantalla, en la que indica 4 puntos principales, basado en:

- Shell
- Reboot
- Cambiar la contraseña del Root
- Cambiar la contraseña del Administrador
- Restaurar por defecto de Fabrica

Algo importante, que se debe tomar en cuenta es que, se debe establecer, es que el endian, debe tener adaptadores de red con diferentes nombres y direccionamiento, en este caso, br0 1: LAN, 192.168.0.15 servidor de seguridad, zona tomate dmz 10.0.0.1, eth2, servidor de correo: 192.168.159.150.

```
Available global commands:

exit                          Exit from the current command.
help                          Help command.
logout                        Logout the interactive shell.
[efw-1382380736] show network> summary
Interface    Zone          Address/Mask       Broadcast       MAC Address
br0          GREEN      192.168.0.15/24   192.168.0.255 00:0c:29:c6:bf:48
br1          ORANGE        10.0.0.1/24      10.0.0.255 00:0c:29:c6:bf:52
br2          -                           -             - e6:a7:7f:0d:36:83
eth0         GREEN                       -             - 00:0c:29:c6:bf:48
eth1         ORANGE                      -             - 00:0c:29:c6:bf:52
eth2         -       192.168.159.150/24 192.168.159.255 00:0c:29:c6:bf:5c
lo           -              127.0.0.1/8 127.255.255.255 00:00:00:00:00:00
[efw-1382380736] show network> _
```

Imagen n°60: Zonas ip

Teniendo, presente cada uno de los acceso a la red que los servidores de la empresa, ahora se genera en direccionar mediante la Ip que brinda el Endian firewall, los proceso de configuración.

Test, Configuración para inicializar el Endian Firewall

Para comprobar que el servidor Endian Firewall y una maquinan x de la empresa, se empieza comprobando la conectividad, en este caso:

1.- Se hace ping al servidor Endian Firewall para comprobar si los equipos se encuentran en red, en este caso, el servidor de seguridad, contiene la IP: 192.168.0.15 como puerta de enlace:

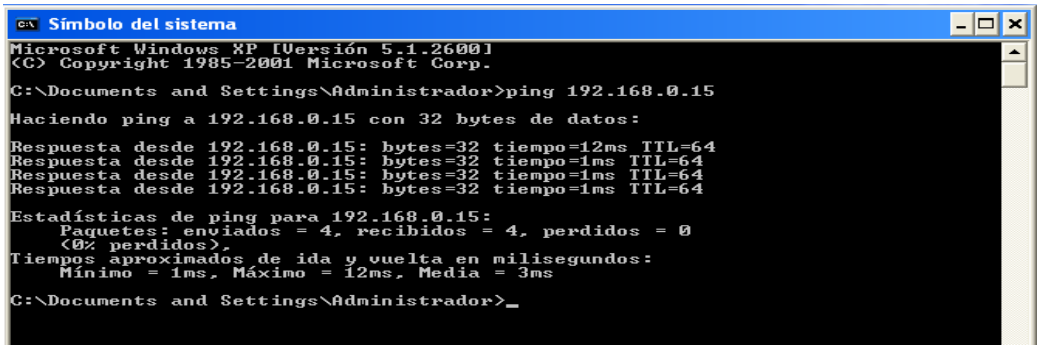


Imagen n°61: Autoría propia del sistema endian firewall, Ping al servidor

Después, se realiza, ping para comprobar si el servidor, se encuentra enlazado a los equipos informáticos de la empresa, en este caso, se toma la Ip, de una de las pcs de la empresa., en este caso:

Se ingresa a Shell, para poder hacer ping a la pc x de la empresa:

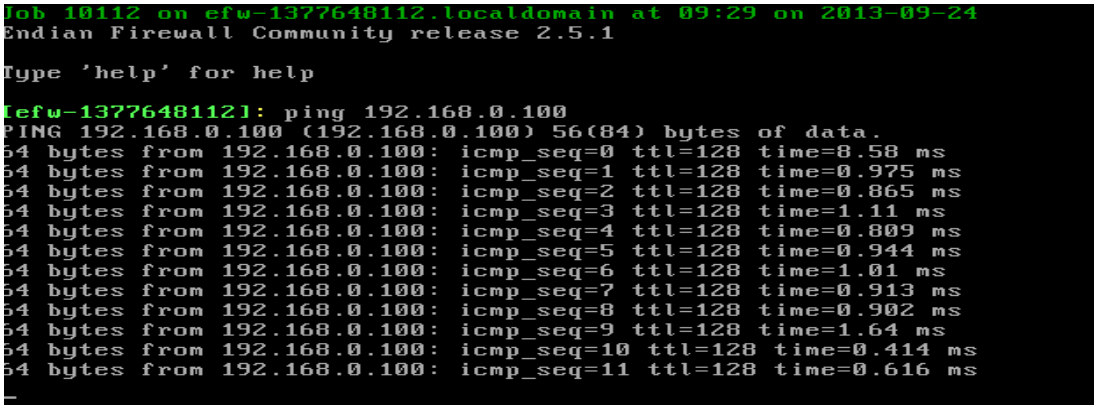


Imagen n°62: Autoría propia del sistema endian firewall, Ping a pc usuario

Las capturas en pantalla, demuestra que tanto, la máquina de la empresa, con el sistema de seguridad Endian Firewall, expone conectividad, para su correcto funcionamiento

CONFIGURACION PARA INICIALIZAR EL ENDIAN DIREWALL

Ingresando al url, que brinda o implementa el firewall, se procede a ingresar mediante la Ip del servidor, basado en la ip segura: 192.168.0.15.

Imagen n°63: Certificado de seguridad endian firewall

A continuación, el siguiente paso, es continuar de todos modos, para poder ingresar a la página de bienvenida para certificar la pagina segura:

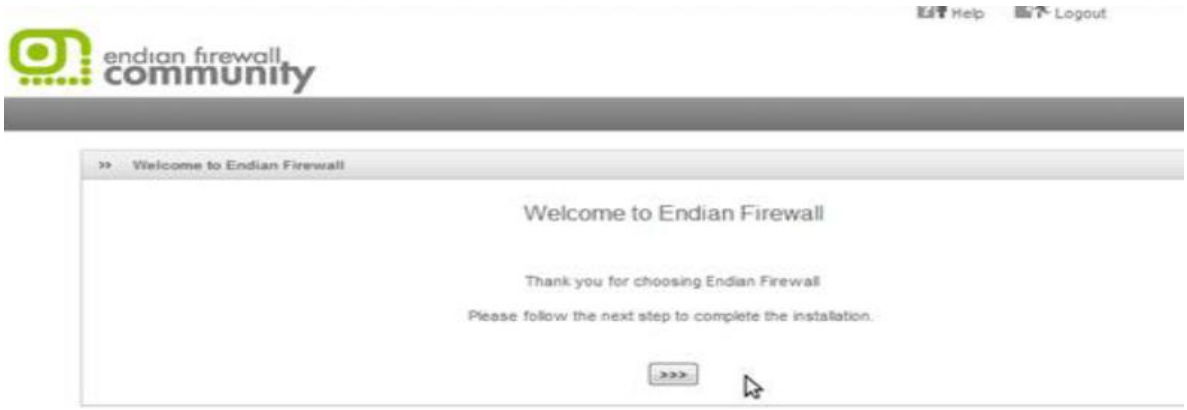


Imagen n°64: Ventana de bienvenida endian firewall

Después de esto, aparece, la selección del idioma y la zona del horario

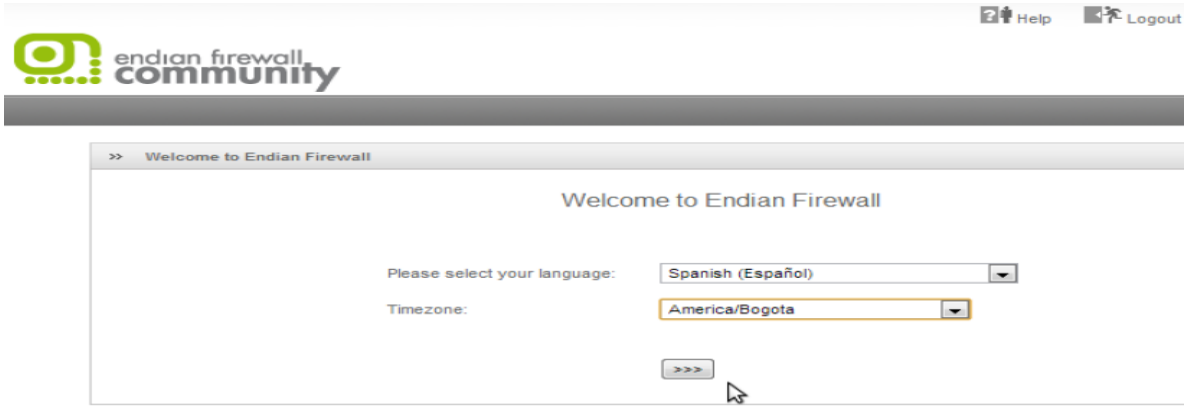


Imagen n°65: Idioma endian firewall

En donde se acepta las condiciones y políticas del Endian Firewall

Imagen n°66: autoría propia del sistema endian firewall

Como no se tiene ningún respaldo, se decide que no, y se procede a seguir:

Imagen n°67: Respaldos endian firewall

Seguido con la parte de las configuraciones, se continúa ahora a ingresar el usuario y contraseña del administrador y acceso root al Sistema Endian Firewall, basado en:

Imagen n°68: Asignación de contraseñas endian firewall

Las contraseñas son:

- Root: 123juan
- Administrador: 123JACOB

Seguidamente, se mostrara en pantalla la ayuda en la selección del tipo de interfaz que se pretende manejar, que hace referencia a los 3 servidores instalados en la empresa: Servidor de Seguridad Firewall, Servidor Fox Pro, Servidor de correo Zimbra.

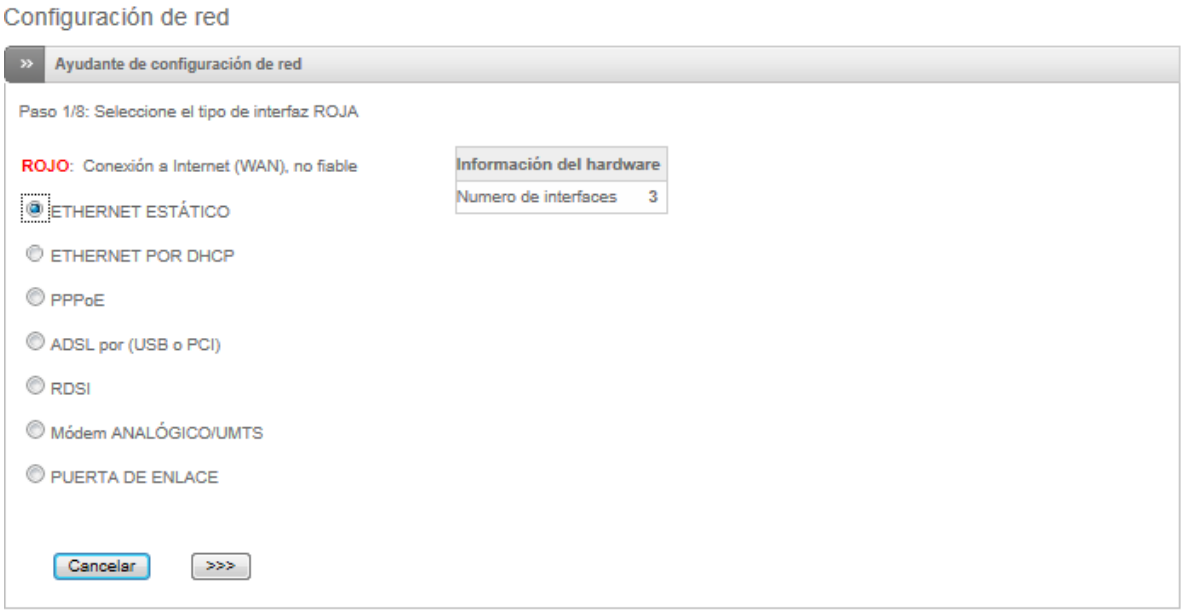


Imagen n°69: Número de interfaces (servidores) endian firewall

Esta parte es importante, ya que indica los tipos de conexiones, como se menciona anteriormente , la red en la Empresa Frada Sport, maneja e incorpora un sistema de IP Fija, basado en establecer Ethernet Estático para poder crear políticas de seguridad, en este caso, se elige la primera opción que es Ethernet estático que representa los diferentes módulos de configuración, dependiendo del tipo de necesidad que represente para la empresa, se puede establecer o generar modelos de desarrollo basados en Dhcp, puerta de acceso, entre otros.

Para la empresa Frada Sport, establece la necesidad de configurar y crear políticas de seguridad basadas en Ips fija, es por esta razón que implementa o configura la Ethernet estática.

Se elige la opción naranja para establecer el segmento de red accesible para los usuarios de internet, es decir se genera otro tipo de servidor interno basado en configurar e instalar

un server DMZ como punto de acceso a los usuarios de la empresa para poder acceder a la Lan interna, y por medio de esta a la wan como puerta de acceso:

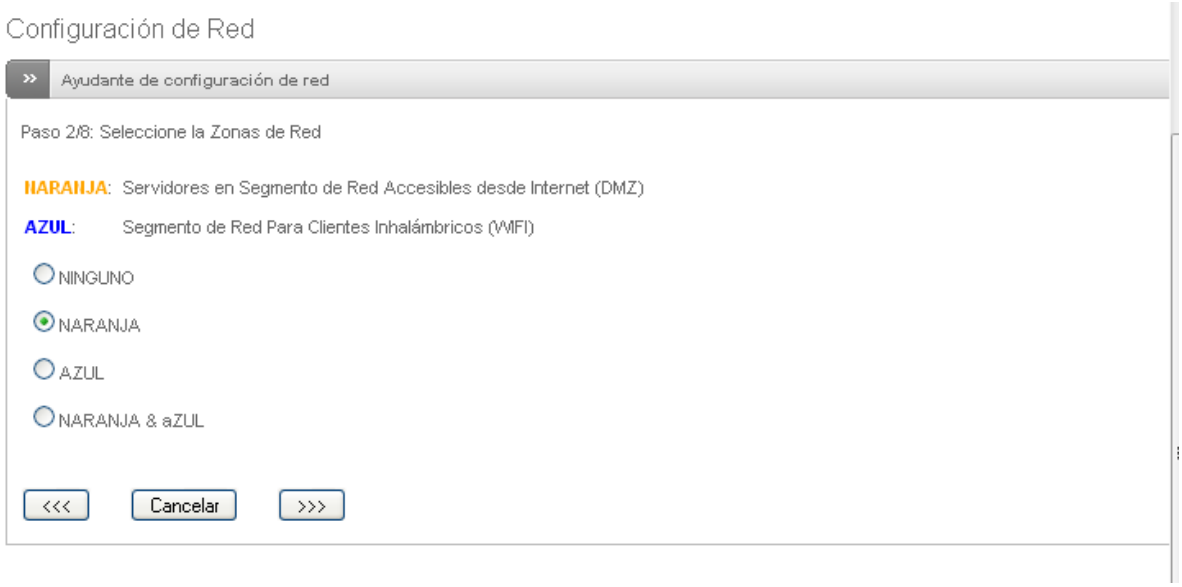


Imagen n°70: Zona desmilitarizada naranja endian firewall

Esta captura de pantalla, que demuestra que el servidor de correo se encuentra en la dirección de Ip indicada.

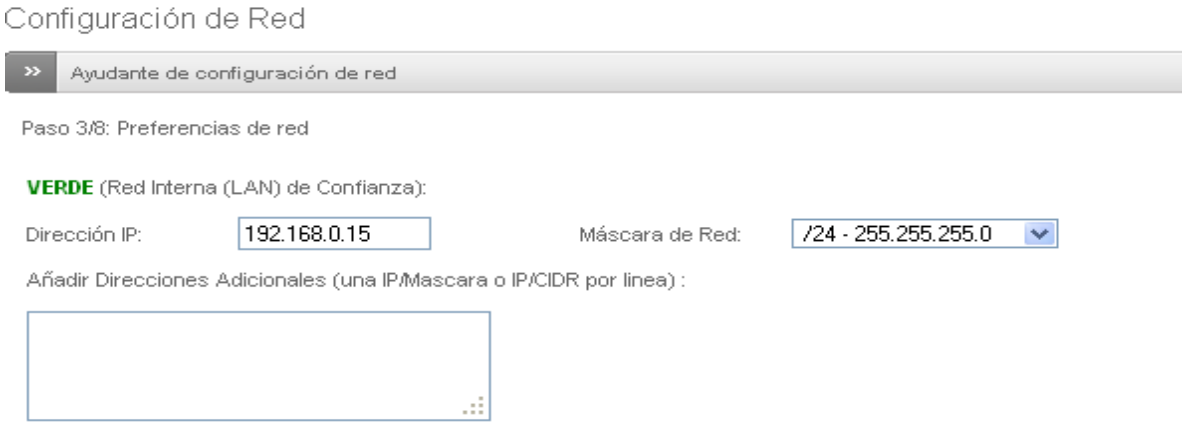
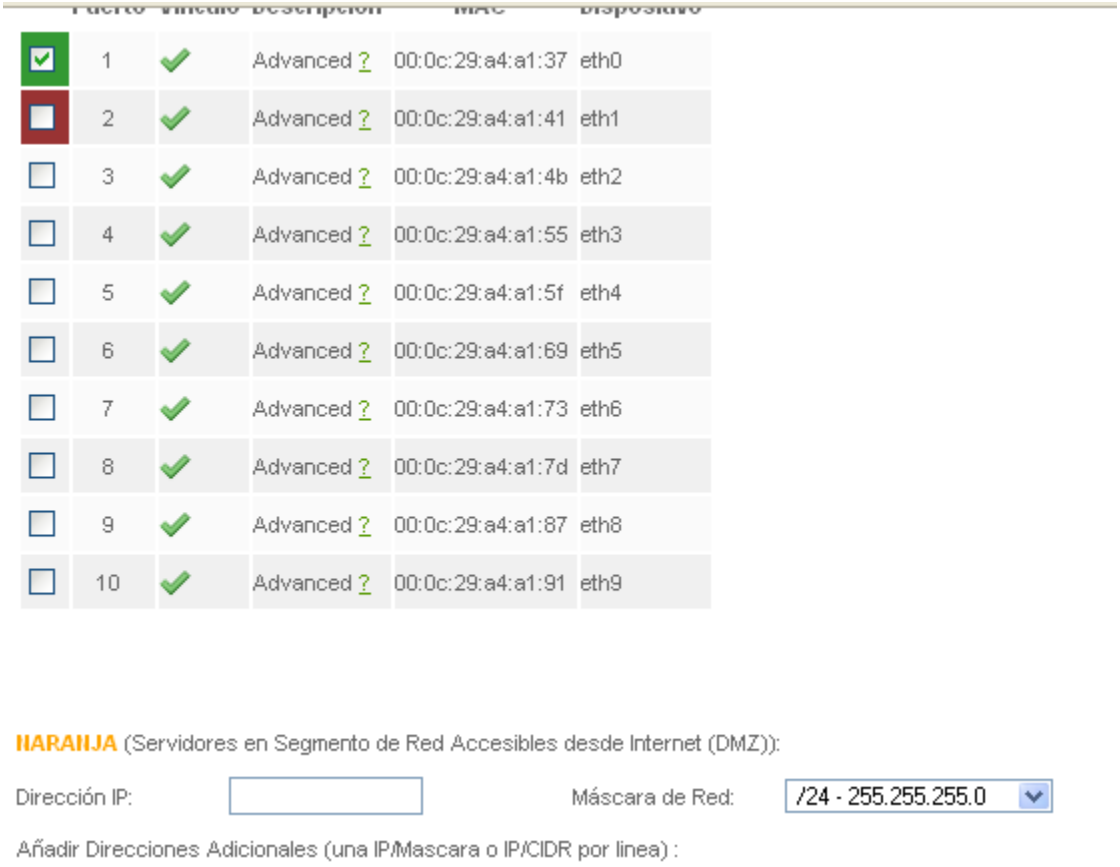


Imagen n°71: Ip zona verde de confianza endian firewall

Aquí se reflejan todas las10 computadoras enlazas y conectadas al sistema de seguridad basadas en establecer acceso a la internet DMZ como zona entrante y saliente de información.



Puerto	Vínculo	Descripción	MAC	Dispositivo
1	✓	Advanced ?	00:0c:29:a4:a1:37	eth0
2	✓	Advanced ?	00:0c:29:a4:a1:41	eth1
3	✓	Advanced ?	00:0c:29:a4:a1:4b	eth2
4	✓	Advanced ?	00:0c:29:a4:a1:55	eth3
5	✓	Advanced ?	00:0c:29:a4:a1:5f	eth4
6	✓	Advanced ?	00:0c:29:a4:a1:69	eth5
7	✓	Advanced ?	00:0c:29:a4:a1:73	eth6
8	✓	Advanced ?	00:0c:29:a4:a1:7d	eth7
9	✓	Advanced ?	00:0c:29:a4:a1:87	eth8
10	✓	Advanced ?	00:0c:29:a4:a1:91	eth9

NARANJA (Servidores en Segmento de Red Accesibles desde Internet (DMZ)):

Dirección IP: Máscara de Red: /24 - 255.255.255.0

Añadir Direcciones Adicionales (una IP/Mascara o IP/CIDR por linea) :

Imagen n°72: Asignación de casillero de dispositivos endian firewall

Teniendo en cuenta esto, se procede a establecer los DNS, en este caso los mismos que Telcocet proporciona a la Empresa Frada Sport:

Imagen n°73: Dns endian firewall

Se aceptan y se aplican los cambios de configuración:

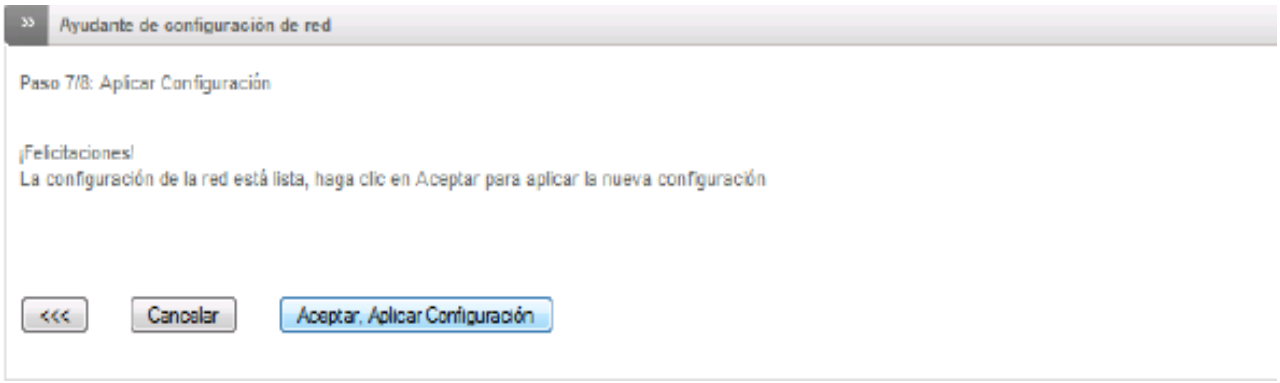
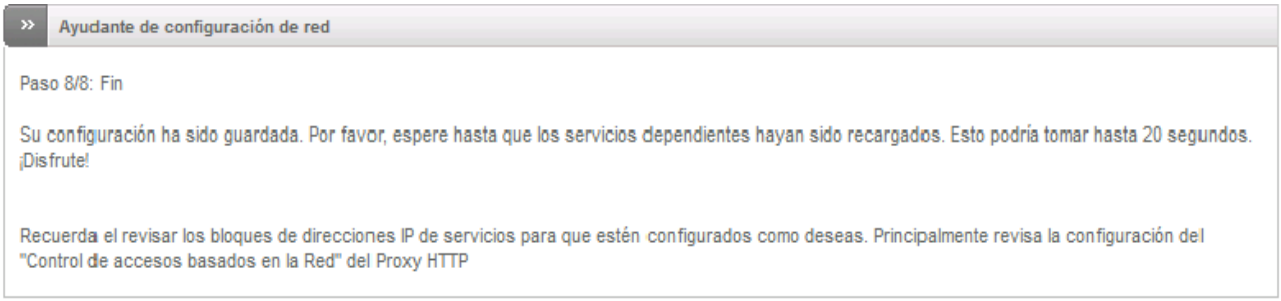


Imagen n°74: autoría propia del sistema endian firewall

Después de haber aplicado todas las configuraciones previamente hechas, el servidor Endian Firewall, se reiniciara automáticamente, esto tarda unos minutos.



En donde el último paso será esperar unos segundos e ingresar nuevamente al sistema:

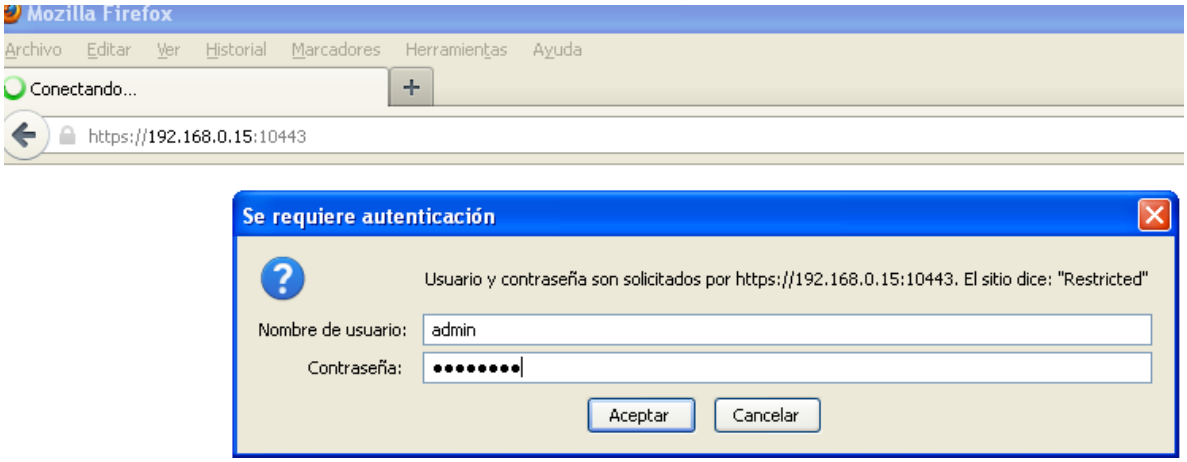


Imagen n°75: Primera ventana accedido al sistema EFW

Después de generar y establecer las configuraciones previas e ingresado al sistema como tal como punto de partida, se muestra en pantalla inicial del servidor de seguridad Endian Firewall en la que se Redirecciona con la Ip segura, basada en la 192.168.0.15:10443.

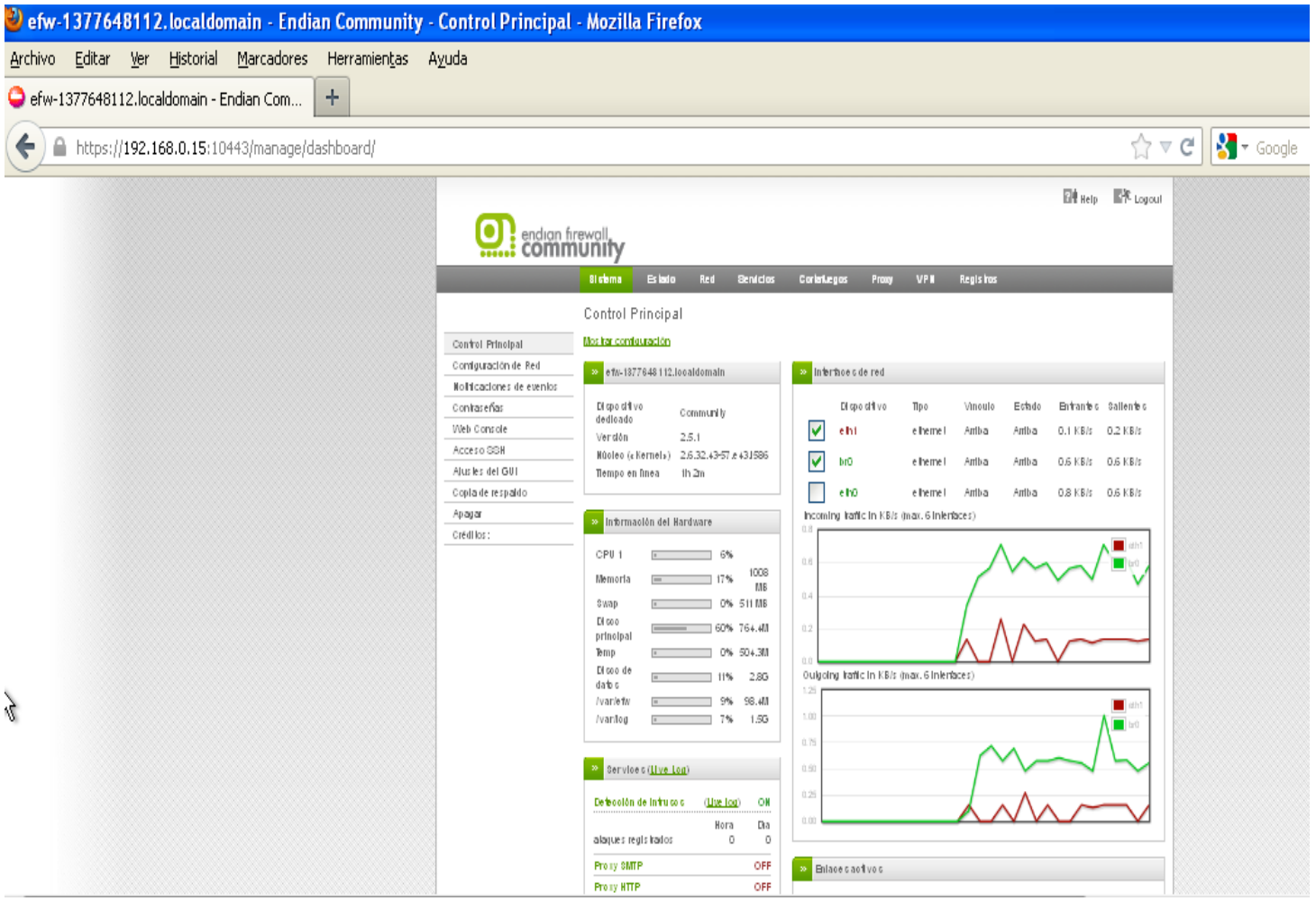


Imagen n°76: Primer ingreso al sistema de seguro EFW

SEGURIDAD ENTRANTE Y SALIENTE DE LA INFORMACIÓN MEDIANTE EL SISTEMA DE SEGURIDAD

(Ver Anexo 2.1)

Activar y configurar el IPS

Esta guía de configuración ilustrará cómo habilitar y configurar el motor de IPS en el Endian.

El primer paso es que el motor IPS haciendo clic en el botón gris (iluminará en verde cuando está activado).

Imagen n°77: Sistema de prevención de intrusos

Después, se despliega una pantalla principal, en donde muestra las siguientes opciones:

Imagen n°78: autoría propia del sistema endian firewall

En esta sección, ejemplifica todas las configuraciones basadas en:

- ❖ Reglas de Amenazas emergentes de SNORT.- Indica que es posible, que las actualizaciones se recuperan automáticamente marcando determinadas casilla.
- ❖ Seleccionar la Agenda de Actualización.- En este punto, se puede seleccionar la programación de actualización, basado en:
- ➢ Horaria
- ➢ Diaria
- ➢ Semanal
- ➢ Mensual

Es importante, en esta configuración, seleccionar el valor por defecto, que se basa en actualizaciones por hora, es decir en cada momento, ya que proporciona una estabilidad y mayor seguridad tanto a los equipos informáticos, como a los servidores propios de la empresa.

- ❖ Actualizar Reglas Ahora.- Esta configuración, hace referencia a, Actualizar e instalar un conjunto un conjunto de reglas iniciales.

Basándose ya en las reglas del Sistema de Prevención de Intrusos, se despliega todo un conjunto de reglas que el sistema como tal examina y escanea.

Es necesario activar cada uno de los puntos que se muestran en pantalla, cada registro, representa y definen un conjunto de reglas muy robusto y estable que permite tener un entorno empresarial seguro.

Se se activa todos los registros de configuración para solventar la seguridad:

Imagen n°79: Reglas snort

El sistema de seguridad Endian Firewall, da la posibilidad si fuese necesario, de eliminar algún registro o editar archivos o reglas SNORT, en este caso:

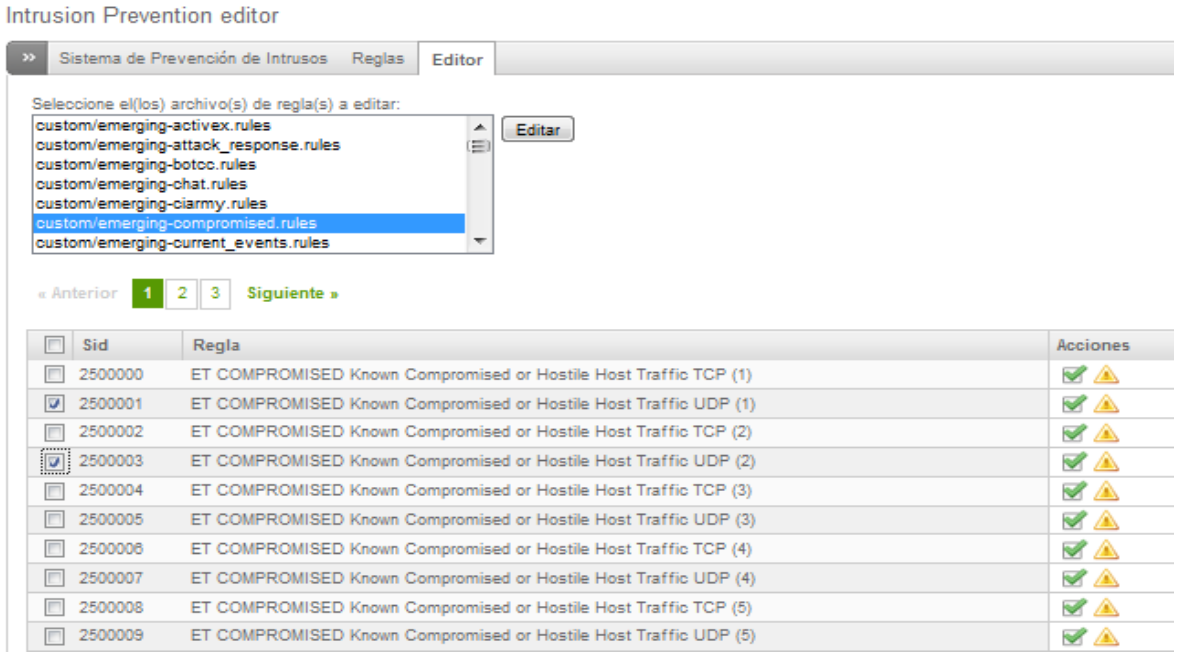
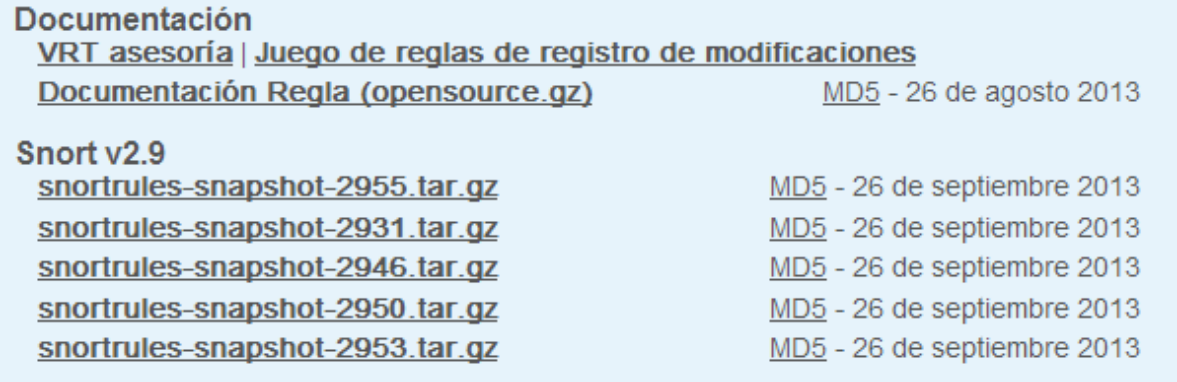


Imagen n°80: edición reglas snort

Reglas Snort Personalizadas

Actualmente las reglas Snort, conlleva una serie de actualizaciones más recientes, de esta manera, el sistema Endian firewall y a su vez, los ISP, muestra que los snort, siempre están en constante cambio evolutivo, basado en mejorar el rendimiento, productividad, fiabilidad y lo más importante, la seguridad de los datos en la empresa Frada Sport.

Es por esta razón, que los SNORT, más recientes se puede descargar de la página oficial como punto de actualización open source.



[29] **Imagen n°81: actualizaciones snort**

Después de proceder si es necesario a las nuevas actualizaciones Snort, se procede a cargar desde el servidor Firewall, haciendo click en examinar y subir reglas ahora.

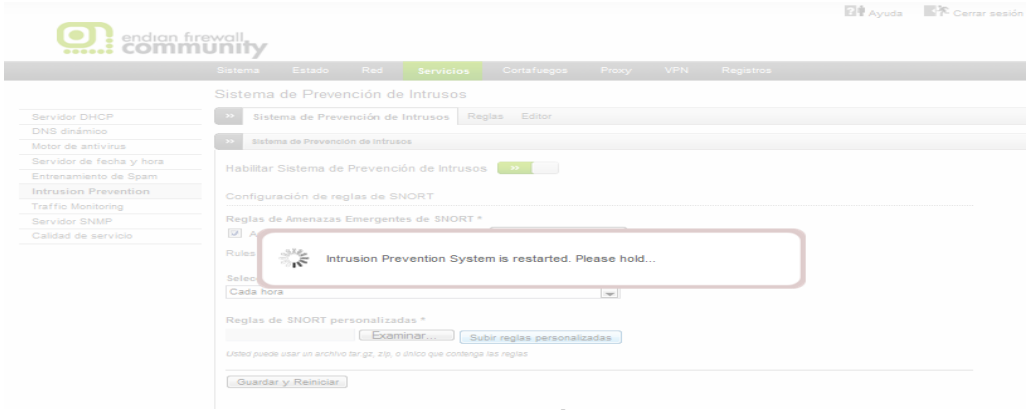


Imagen n°82: Carga ips

Se Espera unos segundos, hasta que los servicios se reinicien e inicialicen, de esta manera las nuevas actualizaciones Snort, quedaran listas de esta manera:

[29] http://www.snort.org/snort-rules/

Imagen n°83: Módulo a llamar ips

Por último, se puede indicar, que los Sistemas de Seguridad, basado en los Snort, conlleva la buena práctica de organización y control de seguridad evolutiva de alta disponibilidad incorporando mecanismos de acciones preventiva y correctiva para la empresa para acciones de prevenir las vulnerabilidades de los diferentes procesos de la misma.

Resultado Saliente

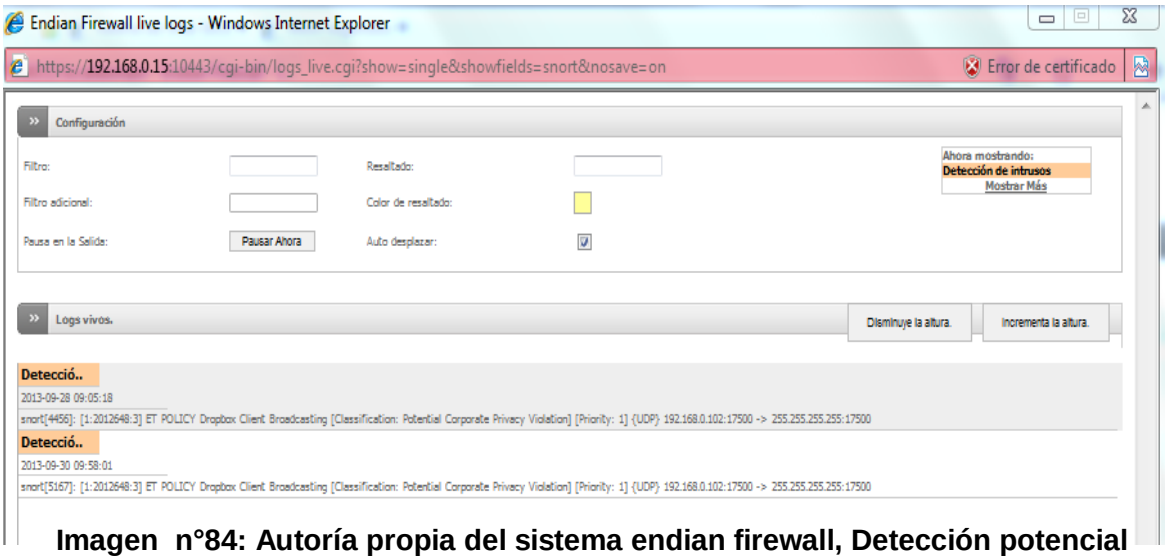


Imagen n°84: Autoría propia del sistema endian firewall, Detección potencial peligroso

Cabe mencionar, que anteriormente, la configuración realizada, basada en escaneo general en busca de programas, archivos, información, o inclusive detección de intrusos, se ve mostrada en la imagen principal.

Como se configura cada hora la agenda de actualización, este caso, se puede constatar que el Snort, encuentra contenido potencial elevado, basado en:

La imagen como tal, muestra en pantalla los denominados logs vivos, en este caso:

Muestra el año, mes y día, basados en las reglas Snort 4456 y 5167, en donde establece e indica un elevado potencial de contenido, en el que también, indica la Ip, que contiene mencionado contenido, en este caso 192.168.0.102, y por último, indica la hora, en las que se manifiesta, 9:05, y 9: 58

CONTROL Y PROTECCIÓN DE LOS DATOS POR MEDIO DE UN ANTIVIRUS Y ANTI.SPAM (MÉTODOS INTELIGENTES) CENTRALIZADOS.

Clamav Antivirus *(Ver Anexo 3.1)*

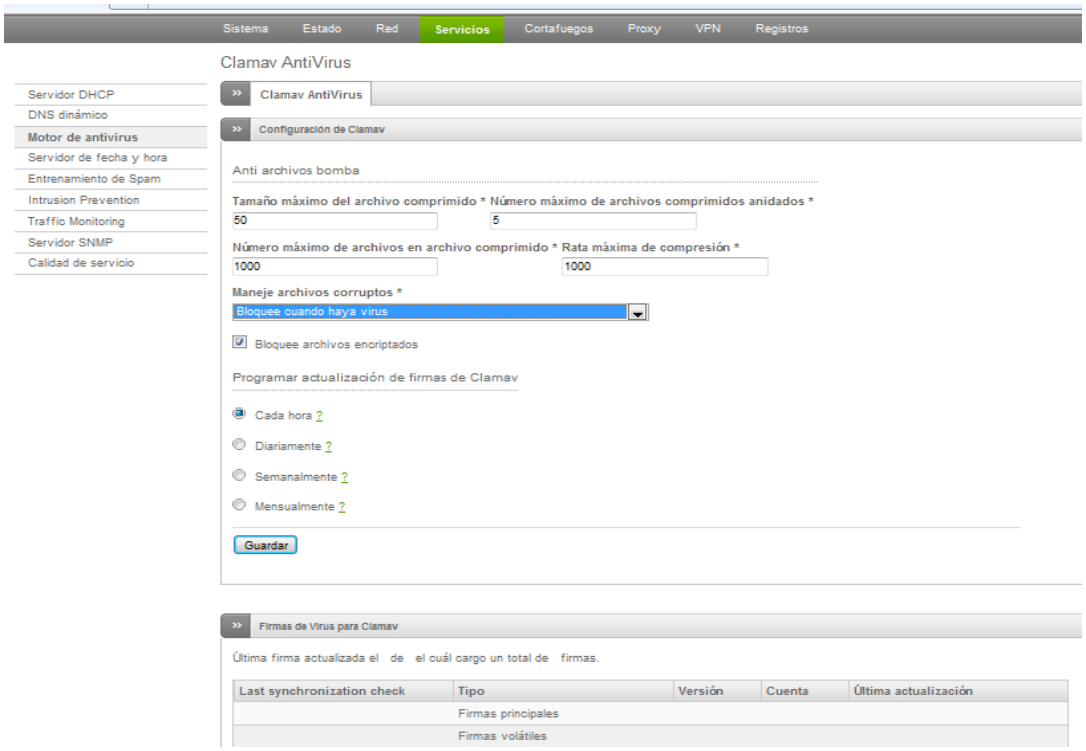


Imagen n°85: Bloqueo virus, clamav

Constituye el motor antivirus de código abierto (GPL) diseñado para la detección de

- Troyanos
- Virus
- Malware
- Otras amenazas maliciosas

- Max. tamaño de archivo[30]

Ajusta el tamaño máximo de archivo en megabytes que se digitalizará por ClamAV.

- Max. archivos anidados

Se especifica la profundidad máxima de archivos anidados ClamAV que explora.

- Max. archivos en archivo

No analizara archivos comprimidos que procesa más archivos que se especifica .

- Relación de compresión máxima

Se especifica la relación de compresión máxima de los archivos que es analizado por ClamAV.

- Se especifica el manejar archivos corruptos, cuando el motor de antivirus encuentra y bloquea cuando exista virus.

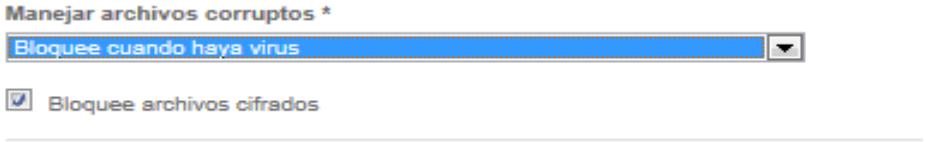


Imagen n°86: Clamav

- Se especifica el tiempo real en la actualización, por cuestiones se seguridad y motor de antivirus actualizado, se procede a establecer en 1 hora.

[30] http://docs.endian.com/archive/2.2/efw.services.html#efw.services.clamav

Imagen n°87: Asignación de actualización

Control de firmas actualizadas, cada cierto periodo de tiempo, se debe estructurar y proceder a generar por medio del motor de antivirus, que las firmas siempre esté actualizado.

Imagen n°88: Firmas de actualización clamav

Y a través del Servidor Proxy, a través del antivirus, se genera una cantidad en Mb, a ser analizado y asignar url de no procesamiento.

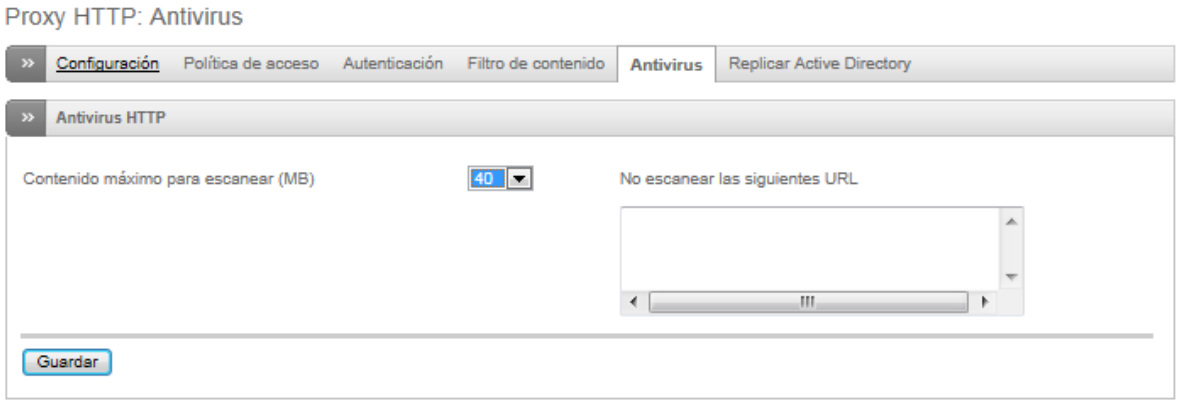


Imagen n°89: Antivirus http

Lo que muestra en pantalla, es simple y únicamente, examina o escanea todos los registros que pasan a través de la red, por lo que el sistema, pregunta cuánto Mb quiere analizar, y en la parte derecha, se puede proporcionar URLs que sean seguras para la navegación de url que manejan los empleados de la empresa, lo más conveniente, como en la imagen es dejar en blanco, para que realice todas las operaciones permitentes de escaneo de toda la red, por lo que se presiona, aplicar y guardar.

Cada política de acceso va a pasar por la configuración del HTTP Habilitar Proxy Http.

En este caso, se habilita el proxy, que gestiona la opción verde de no transparente como medio de política de acceso.

Resultado Saliente

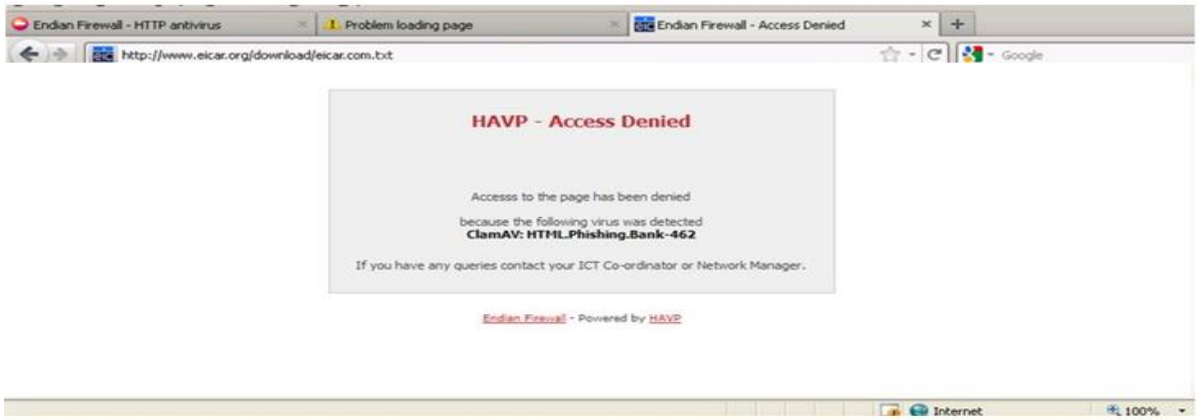


Imagen n°90: Autoría propia del sistema endian firewall, Contenido Pishing

Establece mecanismos de control, basado en bloquear contenidos sospechosos, malicioso, basado en registros phishing, de la web de internet.

Test, el empleado de la empresa, también accede a otras páginas de internet, en donde establece:

Imagen n°91: Autoría propia del sistema endian firewall, Contenido Tojan

Se puede manifestar, que el contenido que presenta la página de internet, posee contenido malicioso, basado en registros troyanos.

Configuración de Proxy

- El puerto que se utilizara será el puerto 8080
- El error del idioma que aparecerá en pantalla, mostrar contenido en ingles.
- El Nombre del equipo visible usado en el proxy será, restricción
- La cuenta de correo usada que se mostrara en pantalla, en asuntos de notificación cache admin será, el correo electrónico, entre otros que por ahora no es importante.

Lo cual se mostrara en pantalla, cada configuración que se crea conveniente e importante para implementar el motor de antivirus central.

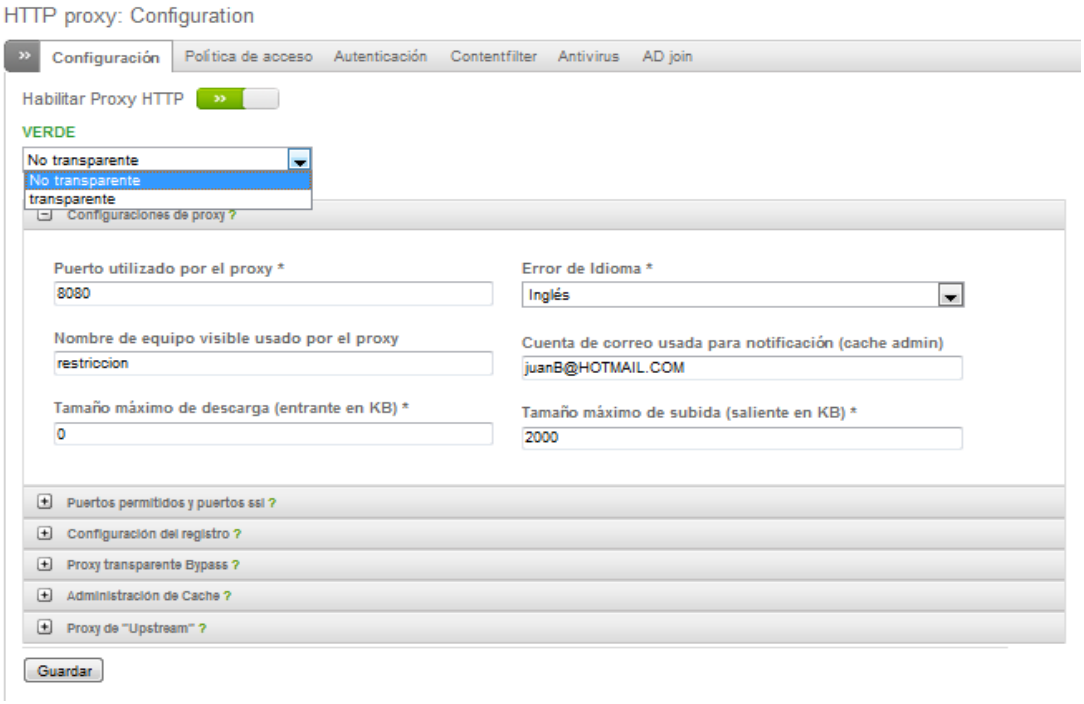


Imagen n°92: HTTP PROXY autoría propia del sistema endian firewall

Se Guarda los cambios pertinentes y se aplica los cambios seleccionados

Proxy No Transparente

En esta parte, es importante tener en cuenta todas las acciones realizadas, el paso siguiente es abrir cualquier navegador, por ejemplo.

Se ejecuta el navegador Mozilla Firefox y se puede navegar de manera total a la web, en este caso:

Imagen n°93: [31]

Entonces, en el navegador, se dirige a Opciones, Avanzadas, Red, Configuración, y se camba la orientación de: sin proxy a configuración manual de proxy: en este caso: 192.168.0.15 que es el servidor EFW, servidor transparente Endian Firewall, de esta manera y usar el mismo proxy para todos los protocolos basados en SS, FTP, Sock, etc.

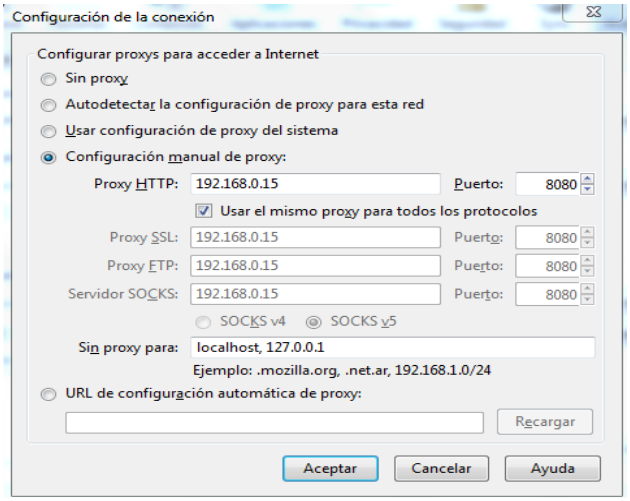


Imagen n°94: Configuración http proxy

Entrenamiento Spam Centralizado *(Ver Anexo 3.2)*

La configuración por defecto no se utiliza para la formación. Todo lo que hace es proporcionar los valores de configuración predeterminados que son heredados por las fuentes reales de formación que se puede añadir a continuación.

[31] www.google.com.ec

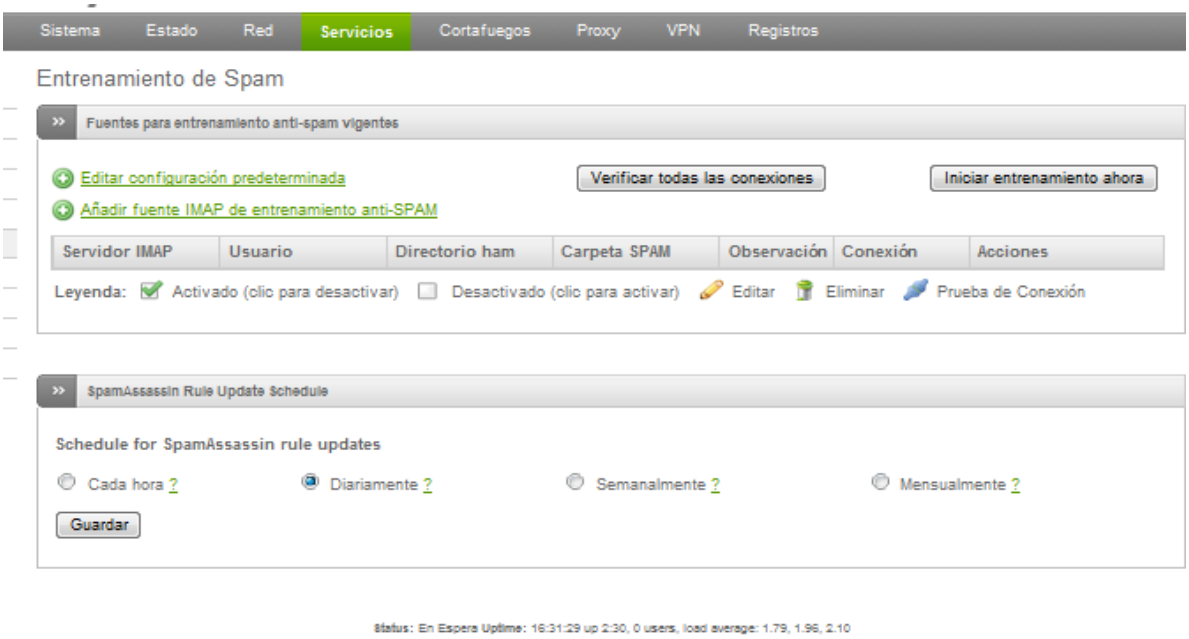


Imagen n°95: autoría propia del sistema endian firewall

Esto puede ser desactivado o ser un intervalo de hora, diario, semanal o mensual. Para obtener información precisa acerca de la hora prevista se puede mover el cursor del ratón sobre el signo de interrogación al lado del intervalo elegido, en este caso, para tener mayor control, lo dejaremos en Diariamente y procederemos a guardar para controles de actualización.

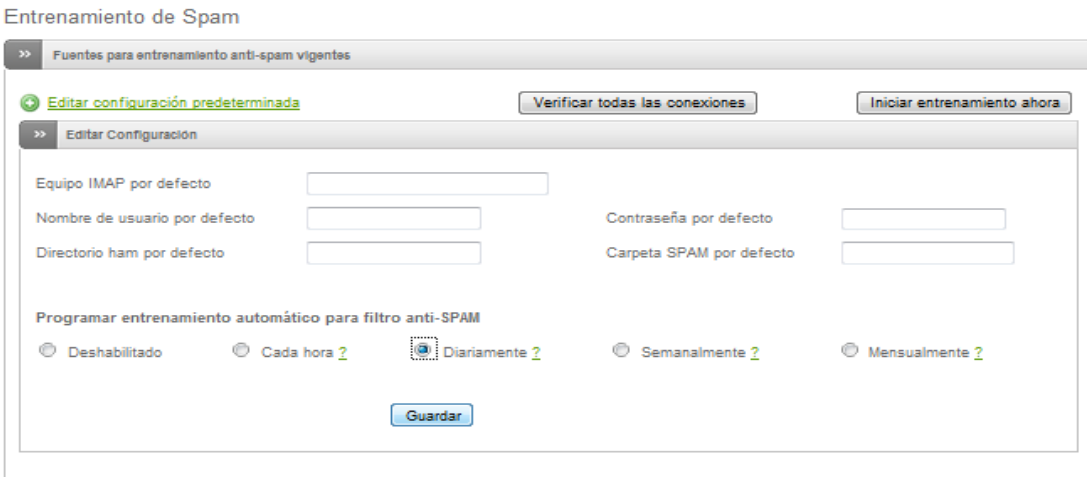


Imagen n°96: Entrenamiento de filtro spam endian firewall

Filtro de Correo No Deseado

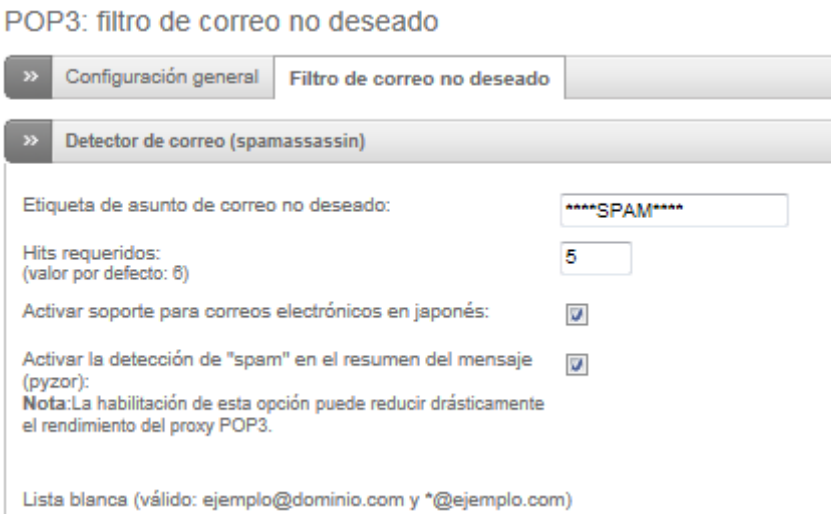


Imagen n°97: Pop 3 filtro de contenido no deseado

Se especifica la etiqueta de asunto de procesamiento spam, se activa la detección de mensajería spam.

Listas blancas y negras personalizadas

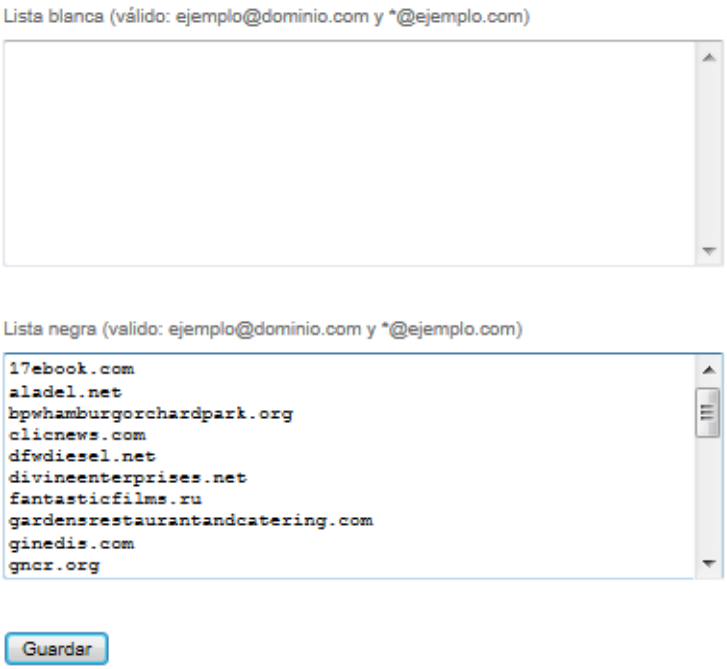


Imagen n°98: Listas blancas y negras personalizadas spam

Se genera a través de las listas blancas y negras personalizadas, un conjunto de páginas webs, que proporcionan o generan mal estar a la hora de acceder a dichas páginas, las urls, destacan contenido no deseado, información basura o maliciosa.

Fuente IMAP de entrenamiento anti-SPAM

Al desplegar esta opción, Agregar IMAP de spam fuente formación, aparece un nuevo panel. Las opciones para los registros adicionales son similares a las opciones de configuración por defecto. Lo único que falta es la programación. Esto siempre se hereda de la configuración por defecto. Tres opciones están disponibles en esta sección.

Los Mails si se marca esta casilla se eliminarán después de haber sido procesado

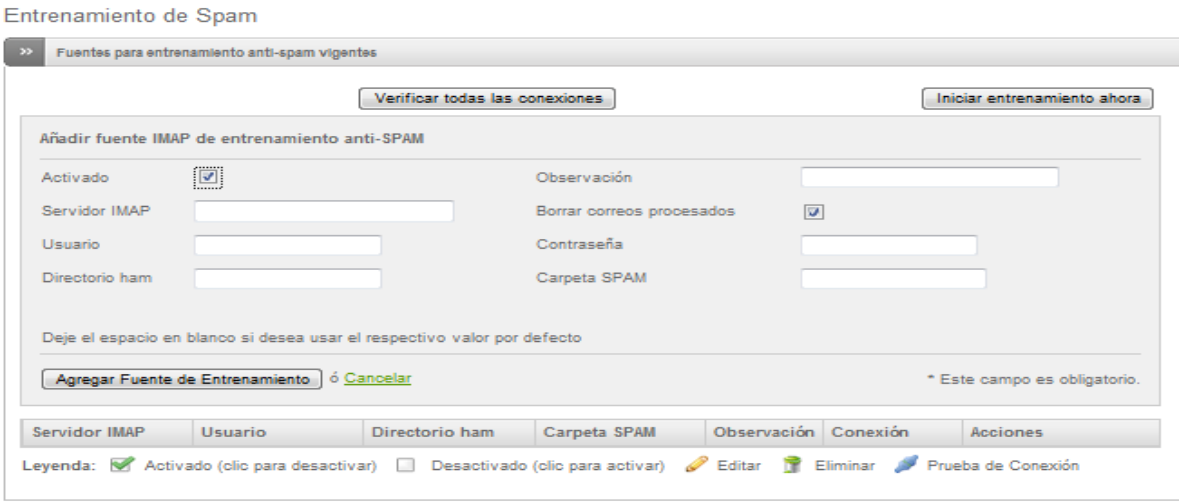


Imagen n°99: Mail de eliminación spam

Es necesario ejecutar el modo entrenamiento, aunque sea un poco demorado, dependiendo del número de fuentes, la velocidad de conexión y lo más importante en el número de mensajes de correo electrónico que se descargarán.

Imagen n°100: Ejecución de entrenamiento spam

SpamAssassin Rule Update Schedule, muestra las actualizaciones que se pueden entrenar en horas, diariamente, semanalmente, mensualmente. En este caso se selecciona diariamente y se procede a guardar los cambios pertinentes.

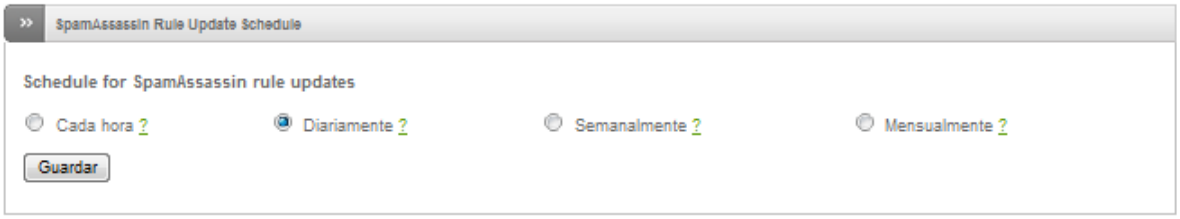


Imagen n°101: Modo de actualización spam

Otra manera de configuración

En la parte de proxy, se selecciona smtp, y se activa el proxy en la sección verde.

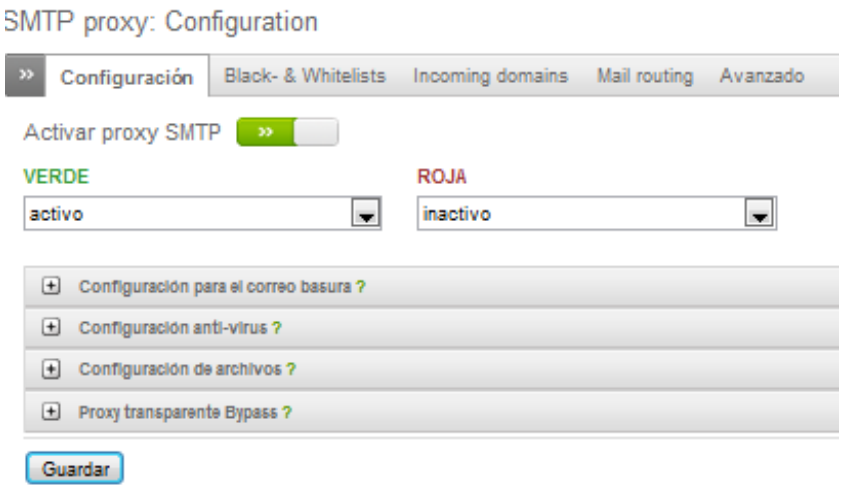


Imagen n°102: Configuración Smtp proxy

Se despliega unas configuraciones, basadas en:

- Elija como manipular el spam
- Se establece en : Dejar como correo basura
- Las demás configuraciones por defecto
- Y se activa el sistema de listas para el correo basura
- Correo usado para las notificaciones, se gestiona en un correo

Si se hace referencia a los denominados Black- & Whitelists, se despliega varias opciones, pero la más importante, en ente campo, tiempo real de listas negras, se puede observar y constatar que cada url que contiene registros spam, los bloqueara.

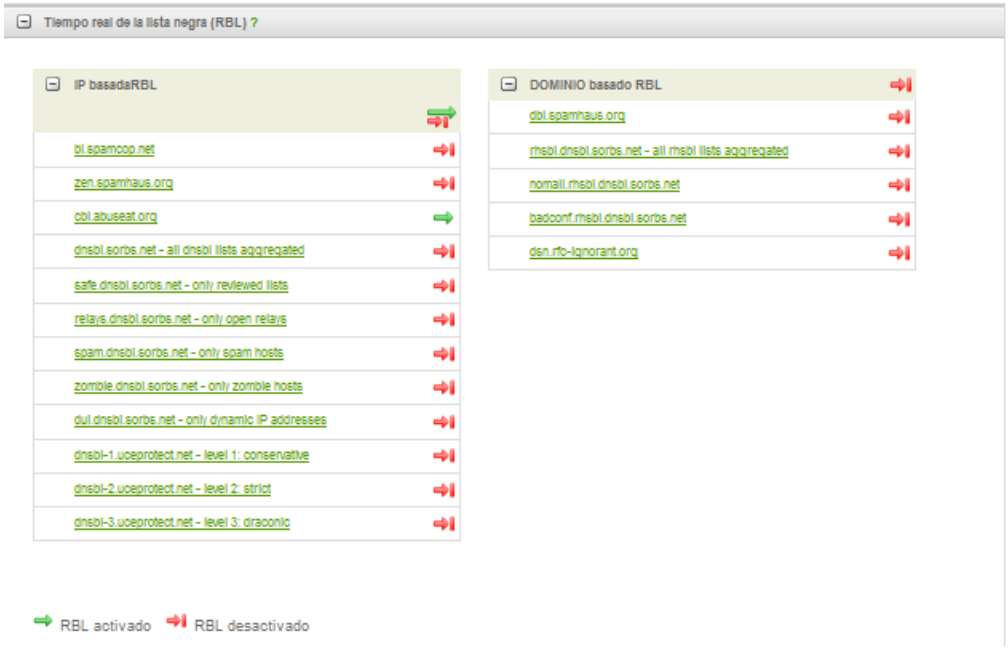


Imagen n°103: Tiempo real listas negras bloqueo

Se procede a Guardar y aplicar los cambios pertinentes

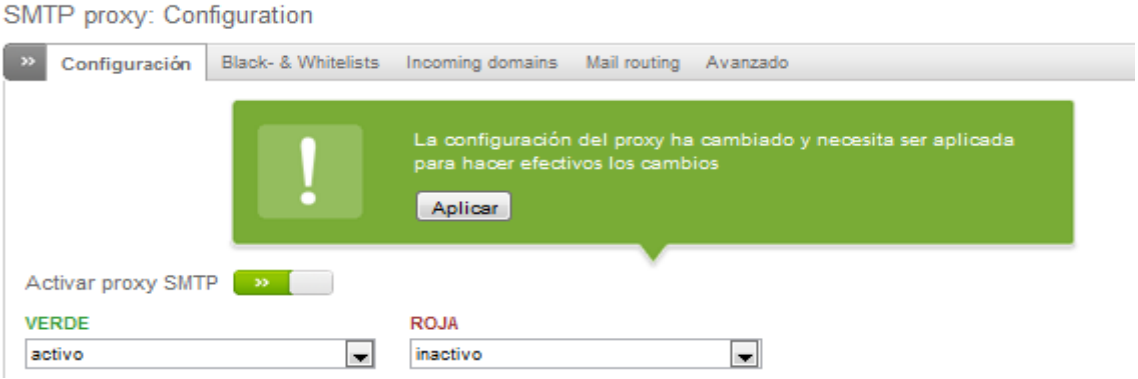


Imagen n°104: autoría propia del sistema endian firewall

Si detecta el control automático de spam por defecto, las acciones que se harán, será de bloquear el contenido, impidiendo y mostrando en pantalla, el acceso al contenido.

La configuración por defecto no se utiliza para la formación. Todo lo que hace es proporcionar los valores de configuración predeterminados que son heredados por las fuentes reales de formación que se pueden añadir a continuación.

Parámetros de configuración Automática o Predeterminada

- *Por defecto IMAP anfitrión*

Anfitrión IMAP que contiene las carpetas de capacitación

- Nombre de usuario predeterminado

Nombre de inicio de sesión para el host IMAP

- La contraseña por defecto

Contraseña del usuario

- Carpeta de jamón por defecto

Nombre de la carpeta que contenga sólo mensajes de jamón

- Carpeta de spam por defecto

Nombre de la carpeta que contiene sólo los mensajes de spam

- Programar una formación filtro de spam automático

FUENTE IMAP DE ENTRENAMIENTO ANTI-SPAM

Este proceso de configuraciones, identifica un nuevo panel. Las opciones para los registros adicionales son similares a las opciones de configuración por defecto. Lo que siempre se hereda de la configuración por defecto. Tres opciones están disponibles en la sección.

- Activado

Se utilizará la fuente de formación cada vez spamassassin se entrena

- Observación

En este campo, es posible ahorrar comentario a recordar el propósito de esta fuente en un momento posterior

- Eliminar mensajes procesados

Los Mails si se marca la casilla, se eliminara después de haber sido procesado

SPAMASSASSIN RULE UPDATE SCHEDULE,

Se determina y muestra las actualizaciones que se pueden entrenar en horas, diariamente, semanalmente, mensualmente, la más común y determinante para la empresa, establece parámetros de configuración diaria.

DISTINTAS MANERAS DE CONFIGURACIÓN SMTP

Las acciones de configuración, se basan en:

- Elegir como manipular el spam
- Se establece en : Dejar como correo basura
- Configuraciones por defecto
- Se activa el sistema de listas para el correo basura
- Correo usado para las notificaciones, se gestiona en un correo

Si se hace referencia a los denominados Black- & Whitelists, muestra varias opciones, pero la más importante, en dichos procesos, es tiempo real de listas negras, basados en url que contiene registros spam.

Decir también, que si se detecta el control automático de spam por defecto, las acciones que se harán, será de bloquear el contenido, impidiendo y mostrando en pantalla, el acceso al contenido.

Resultado Saliente

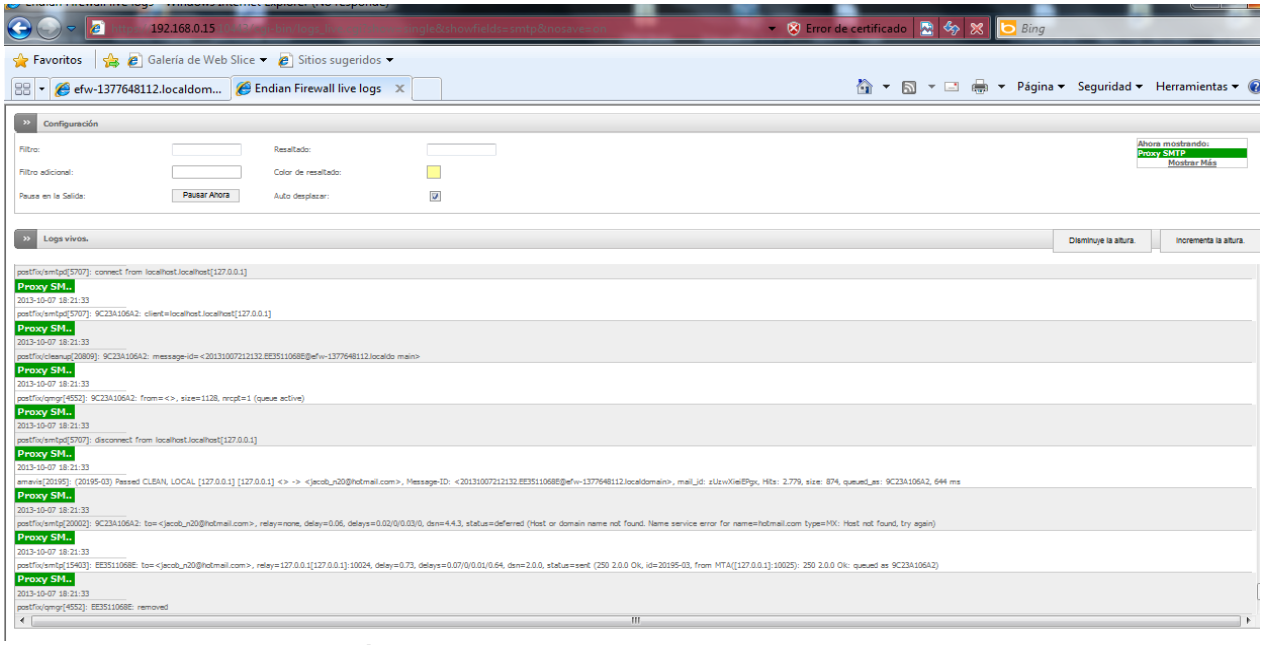


Imagen n°105: Autoría propia del sistema endian firewall, Logs Vivos SMTP

- Primeramente se conecta al servidor, y capta el proxy transparente, basado en 127.0.0.1
- Identifica claramente al usuario cliente en el localhost, basado en el proxy
- Captura, y muestra en pantalla el mensaje lógico con un serial o registro único.
- Algunos registros, indica que este usuario se desconecta.
- Podemos también destacar, que este usuario que vuelve a conectar , y uno de los aspectos más importantes, establece el correo electrónico de la persona o usuario de la empresa que contiene registros o mensajes spam

Lo que da la posibilidad de contar con un sistema de ayuda, para identificar mensajes o contenido spam dentro de la red global de la empresa.

MEJORAR EL RENDIMIENTO DE LOS EQUIPOS Y DE LA RED

(Ver Anexo 4.1)

Para efectuar el mejor rendimiento de los equipos informáticos y de la red, se establecen parámetros de accesos de configuración basados en:

- **RED:**

1.- Configuración de Anfitrión o añadir equipos a la red

- **PROXY HTTP:**

1.- Configuración del Proxy

2.-Autenticacion

3.- Contenido de Filtros

4.- Política de Acceso

De manera general sin aplicar todavía políticas de control de acceso segmentado a la red para los usuarios determinados, primeramente se efectúan parámetros de configuración previa, basados en:

- **RED:**

1.- CONFIGURACIÓN DE ANFITRIÓN O AÑADIR EQUIPOS A LA RED

Imagen n°106: Asignación de equipos en la red global

Primeramente se crea o se añade usuarios a los equipos informáticos, basados en:

- ✓ Direcciones IP
- ✓ Nombre de equipo
- ✓ Nombre de Usuario

Lo que se hace en este caso, es añadir los 10 puntos o usuarios de la empresa Frada Sport como punto de partida.

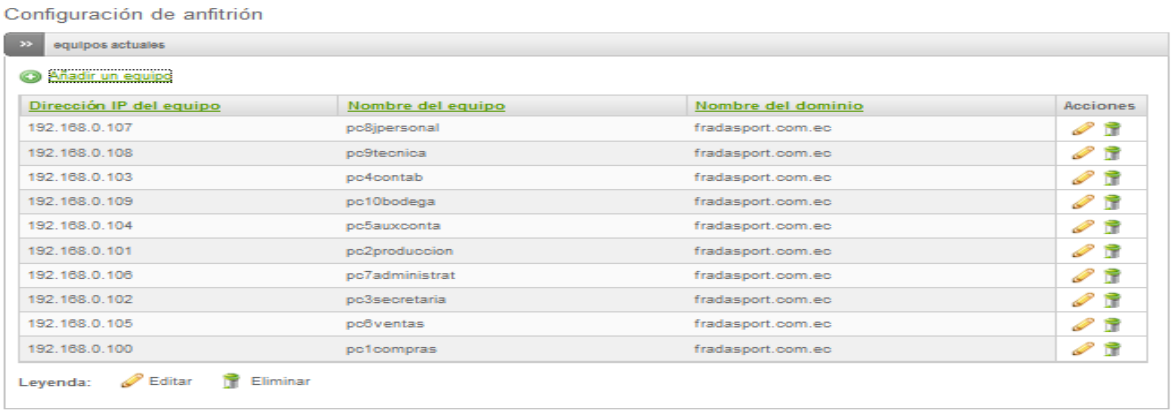


Imagen n°107: Usuarios cargados, endian firewall

- **PROXY HTTP:**

1.- Configuración del Proxy *(Ver Anexo 4.2)*

CONFIGURACIONES DE PROXY:

- Parámetros de configuración:
- Puerto de acceso: 8080
- Nombre de equipos visible usando el proxy: Restricción
- Error en el idioma: Ingles
- Cuenta de correo usada para notificaciones: jacob_n20@hotmail.com
- Tamaño máxima de descarga KB: 0
- Tamaño máximo de subida KB: 0

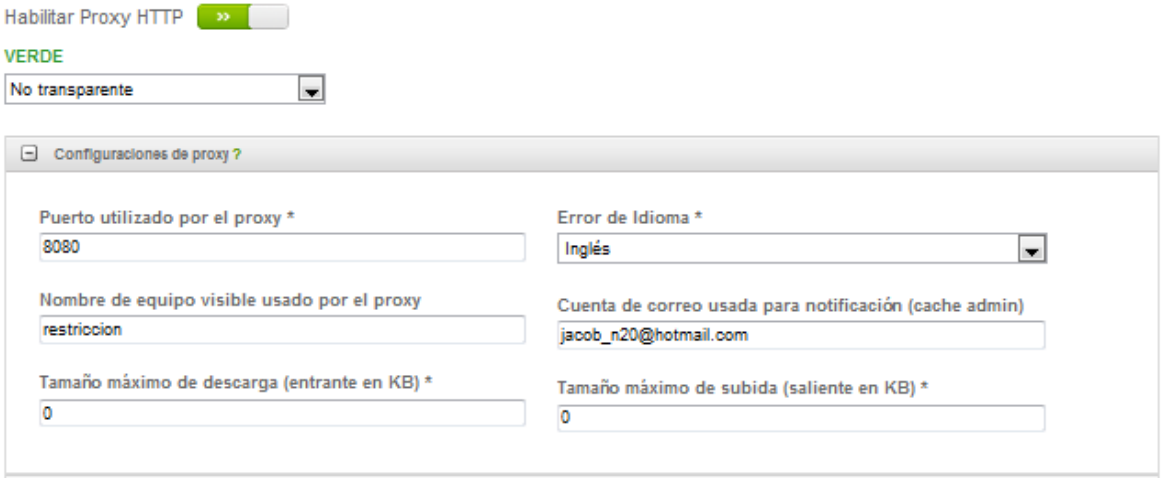


Imagen n°108 Tamaño de subida y descarga bloqueado, endian firewall

PUERTOS PERMITIDOS:

Los puertos que se muestra en pantalla, establecen accesos a las diferentes páginas web, establecidas mediante, si uno de ellos no se establecen en pantalla, simplemente no se accederá a los diferentes puertos de enlace definidos:

- Puerto 80 http
- Puerto 21 ftp
- Puerto 70 gopher
- Puerto 210 wais
- Puerto 280 http-mgmt

Imagen n°109: Puertos permitidos endian firewall

CONFIGURACION DE REGISTROS

Es necesario marcar cada una de las casillas en blanco para crear puntos de registros, basados en:

- Habilitar registro
- Registro de filtro de contenido
- Registro de agente de usuario
- Firewall logging

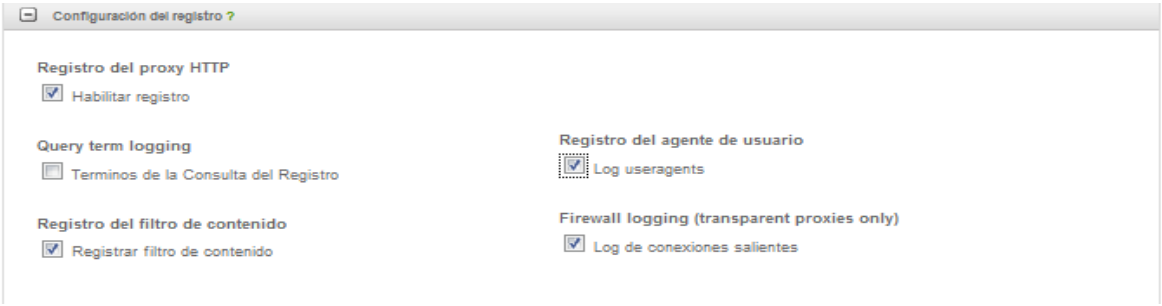


IMAGEN N°110 Configuración de registros proxy

Evitar proxy transparente

Hace referencia a seleccionar y asignar procesos de acceso total a medios de información.

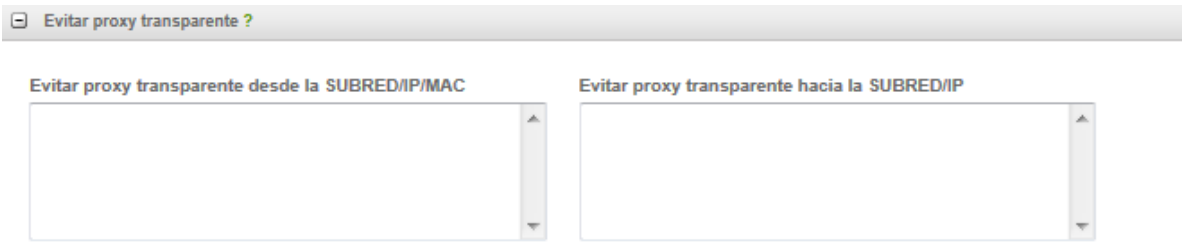


Imagen n°111 autoría propia del sistema endian firewall

Administración de la cache

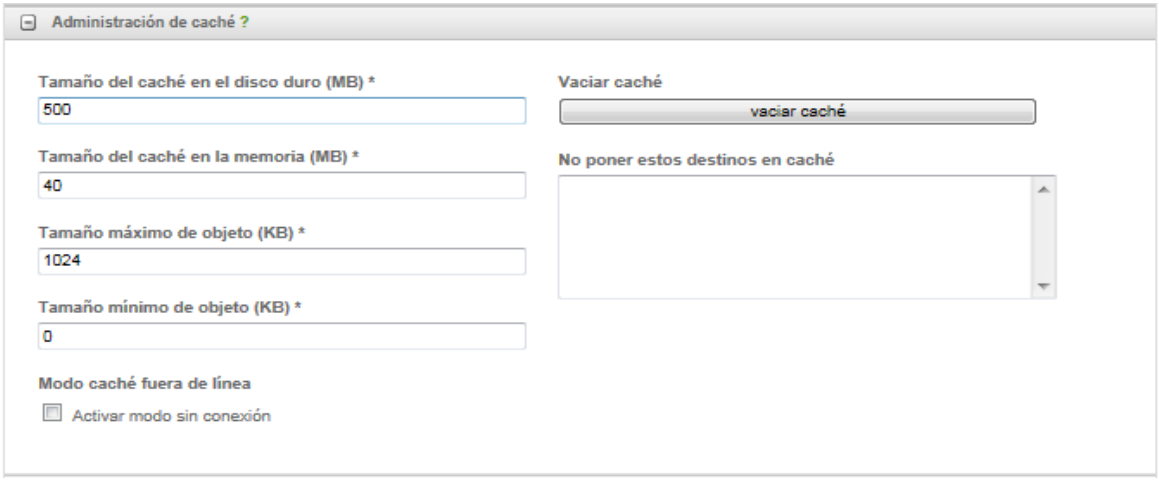


Imagen n°112 Administración cache, endian firewall

Hace referencia al tamaño de especificación que guarda o almacena contenido máximo y mínimo en Mb, también en el proceso de eliminar o vaciar información chache.

2.-AUTENTICACION *(Ver Anexo 4.3)*

Aplicado a las siguientes áreas de la Empresa:

Área Compras
Área Producción
Área Secretaria
Área Contabilidad
Área Auxiliar Contabilidad
Área Ventas
Área Administrativa
Área Jefe Personal
Área Técnica y Tecnológica
Área Bodega

PROXY HTTP AUTENTICACIÓN

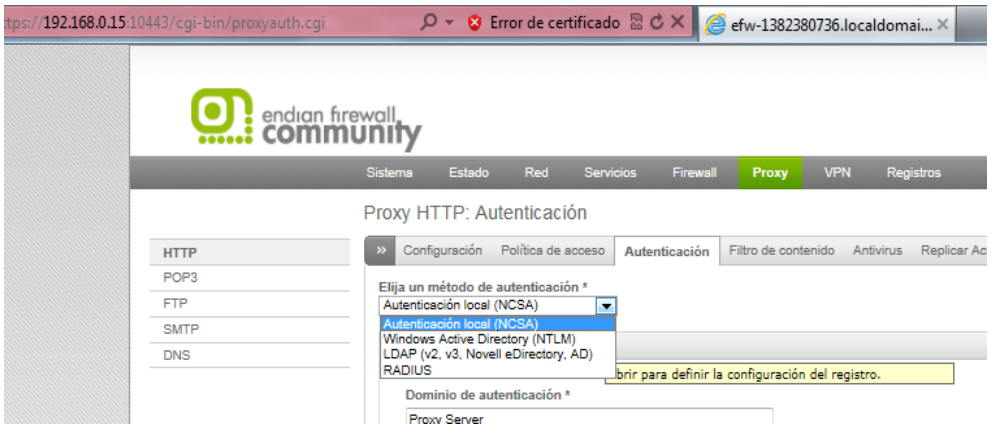


Imagen n°113 Autenticación NCSA

Se asigna y se seleccionar el mejor método de autenticación que incorpora el sistema de seguridad basado en la autenticación NCSA.

Configuración de Autenticación

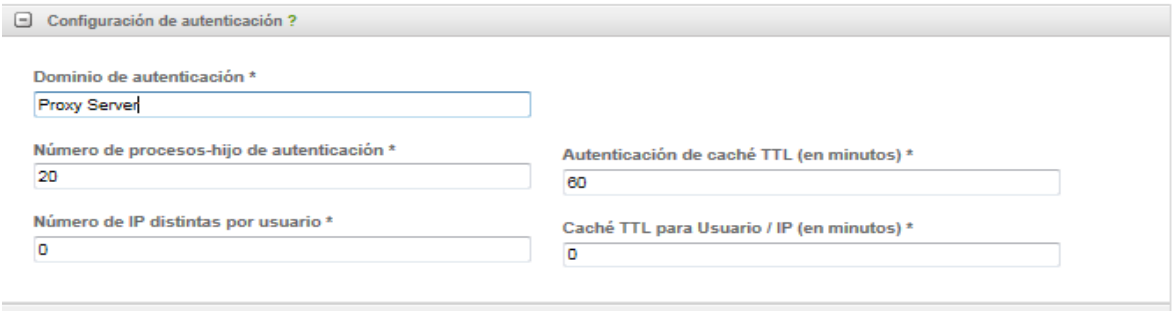


Imagen n°114 Proxy autenticación

Se asigna un nombre o dominio para la autenticación, en este caso, proxy server, sea asigna un tiempo de cache para el acceso por medio de usuario y contraseña.

Configuración especifica de NCSA

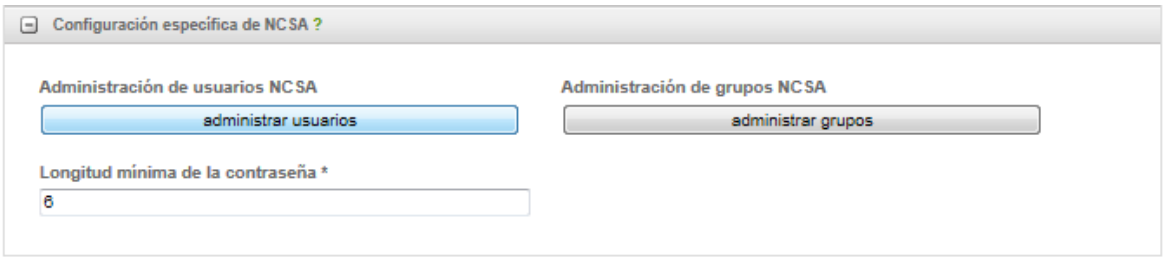


Imagen n°115 Autenticación, administración de usuarios

El método de autenticación NCSA, incorpora procesos de administración por usuario y por grupos, cualquiera de ambas maneras se puede especificar medios de autenticación, y por último se asigna una longitud mínima para la contraseña, en este caso, longitud de 6.

Asignación de usuario y contraseña:

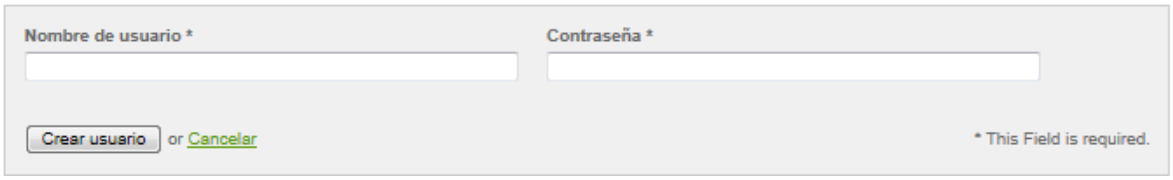


Imagen n°116 Autenticación, asignación de usuario y contraseña

Asignación de usuario y contraseña a cada empleado:

Imagen n°117 Autenticación, usuarios cargados

Todos los usuario de la empresa Frada Sport, cuentan con usuario y contraseña, para obtener control y organización en toda la red global de datos.

Ejemplificación:

Empleado Compras

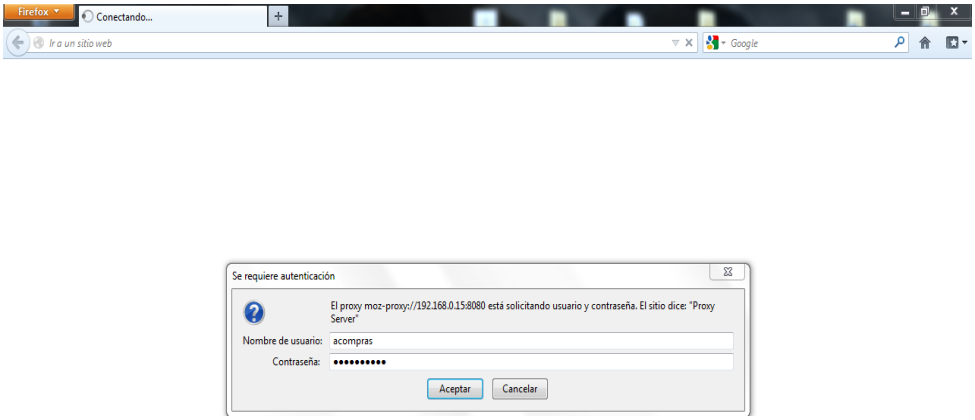


Imagen n°118 autoría propia del sistema endian firewall

Empleado Ventas

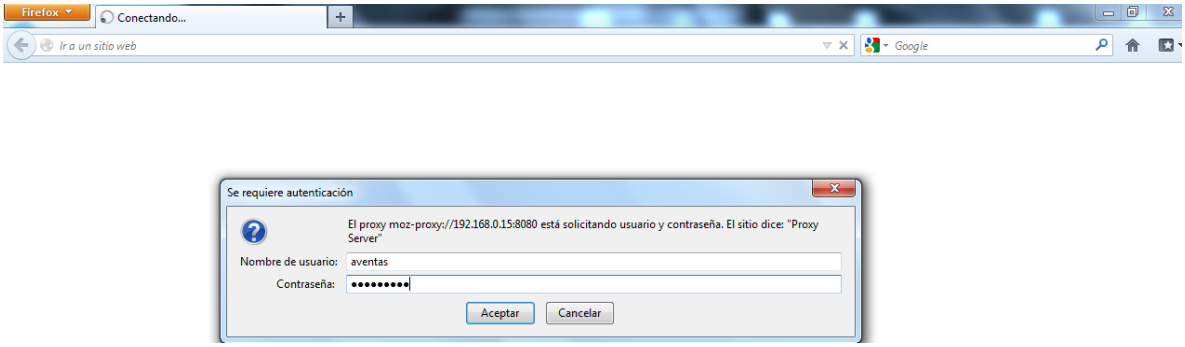


Imagen n°119 autoría propia del sistema endian firewall

Empleado Bodega

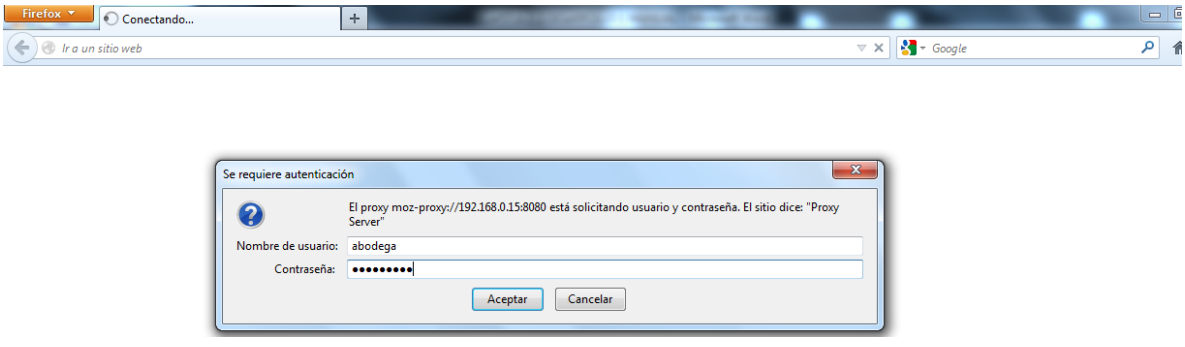


Imagen n°120 autoría propia del sistema endian firewall

3.- CONTENIDO DE FILTROS *(Ver Anexo 4.4)*

DENEGAR ACCESO TOTAL A INTERNET *(Ver Anexo 4.5)*

Aplicado a las siguientes áreas de la Empresa:

Área Compras
Área Secretaria
Área Ventas
Área Técnica y Tecnológica
Área de Bodega

De acuerdo a la segmentación de la red global en la empresa, las áreas destinadas al no acceso al sistema, establece medios de seguridad que no se involucra con la necesidad del uso del internet de ciertas áreas de trabajo, basado en:

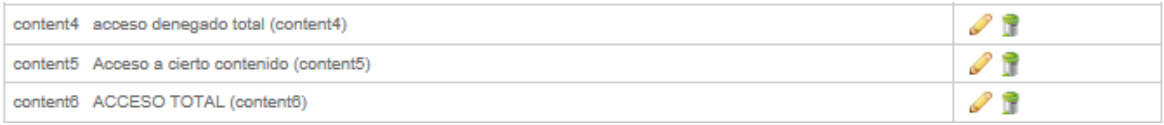


Imagen n°121 Contenido de filtros

Imagen n°122: Filtro acceso denegado total.

Se puede apreciar en la imagen, los filtros que hacen referencia a contenido por categorías, y filtros de paginas establecidas en acceso url, en la parte derecha, indica la flecha roja, que está bloqueada.

Filtros de páginas que contienen frases de las siguientes categorías. (Filtrado de contenidos)

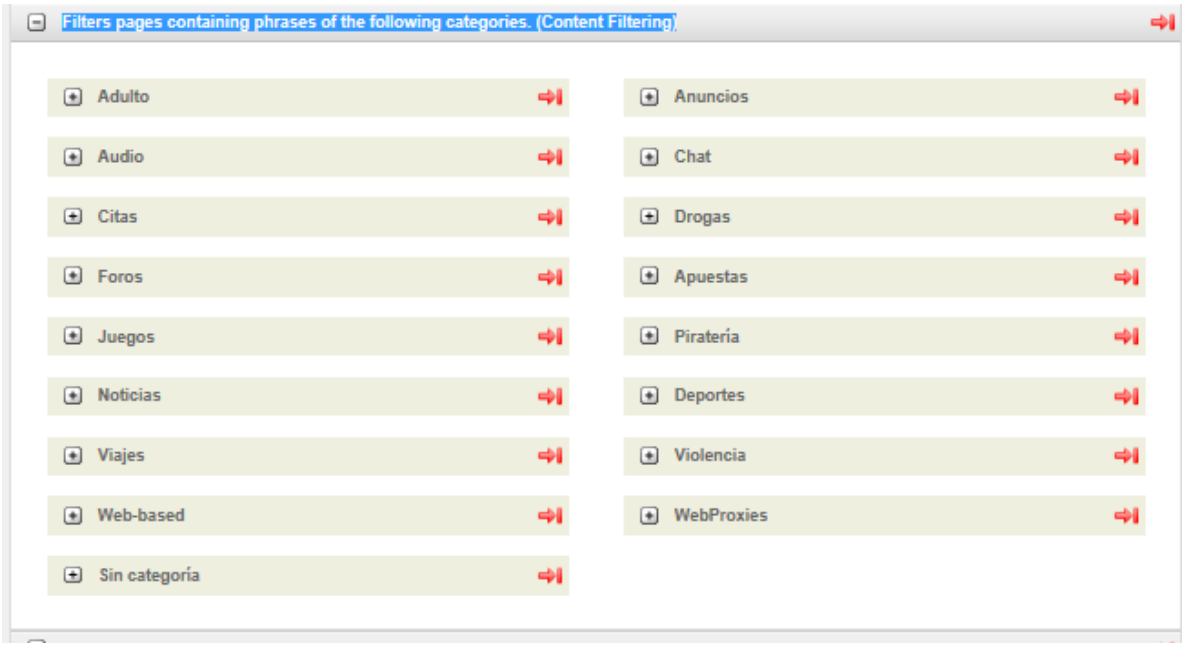


Imagen n°123 Contenido de filtro de páginas web

Todo este comprendido de categorías de páginas, indica que cada sección esta bloqueada, ya sea contenido adulto, de audio, de juegos, de chat, deportes, entre otros.

Dentro de cada categoría, se despliega más contenido por categoría, en donde también es bloqueado

Imagen n°124 Contenido de filtro de páginas web

Las mismas acciones, se ven reflejado en:

Páginas de filtros de contenido de las siguientes categorías URL

Imagen n°125 Contenido de filtro url

Se aplica las mismas acciones, referente a paginas url, de la misma manera, todo el conjunto de páginas, será bloqueado.

Dentro de cada página, se despliega más contenido por web url, en donde también es bloqueado

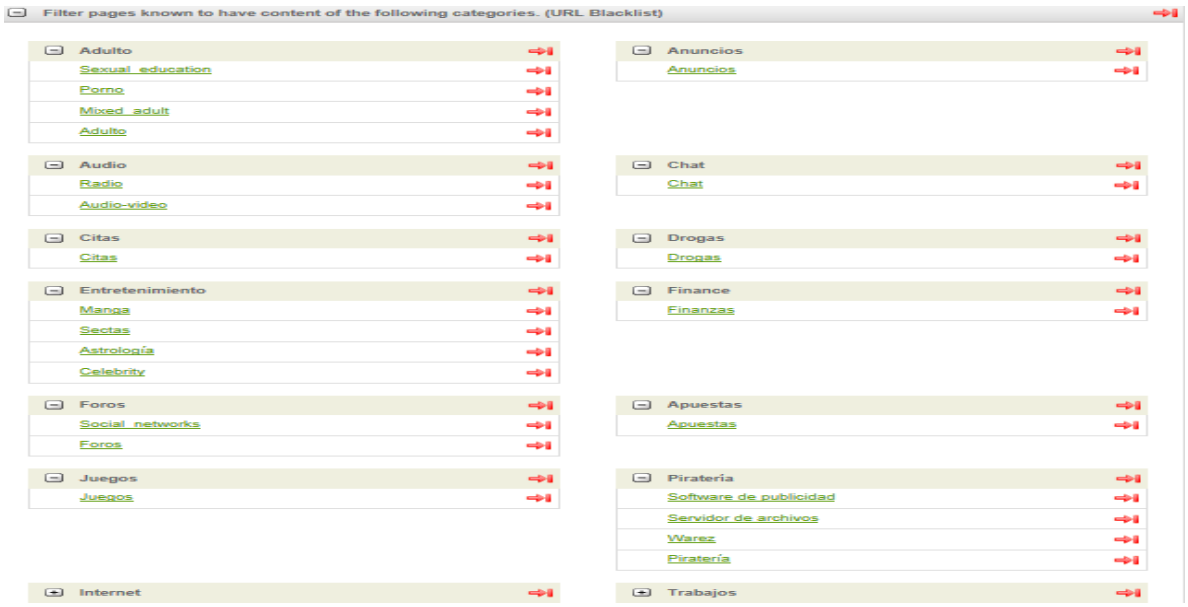


Imagen n°126 Contenido de filtro url

Listas negras y blancas personalizadas.

En este apartado, las configuraciones para los diferentes medios de acceso, no involucra ningún contenido de páginas, ya que solo están establecidas, bloquear páginas por categoría y url.

Resultado Saliente:

Google.com

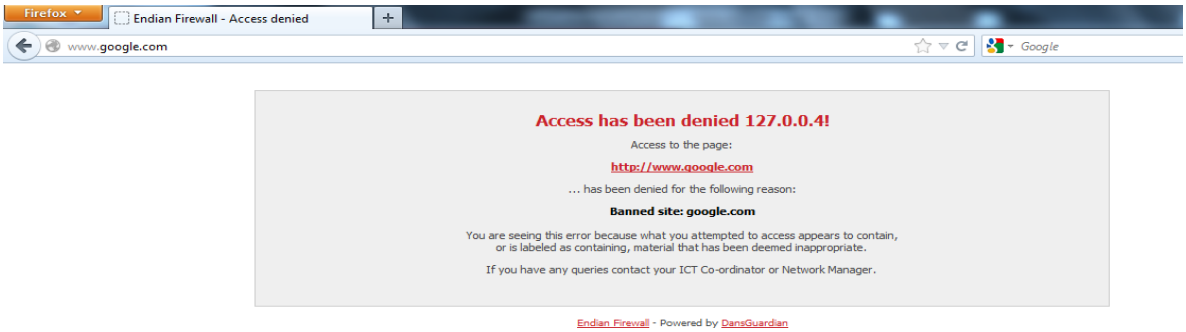


Imagen n°127 autoría propia del sistema endian firewall

Email.

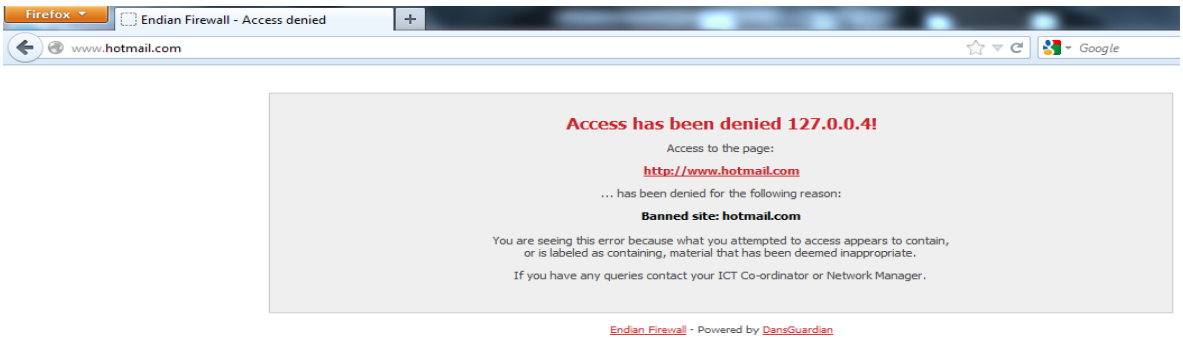


Imagen n°128 autoría propia del sistema endian firewall

Gmail

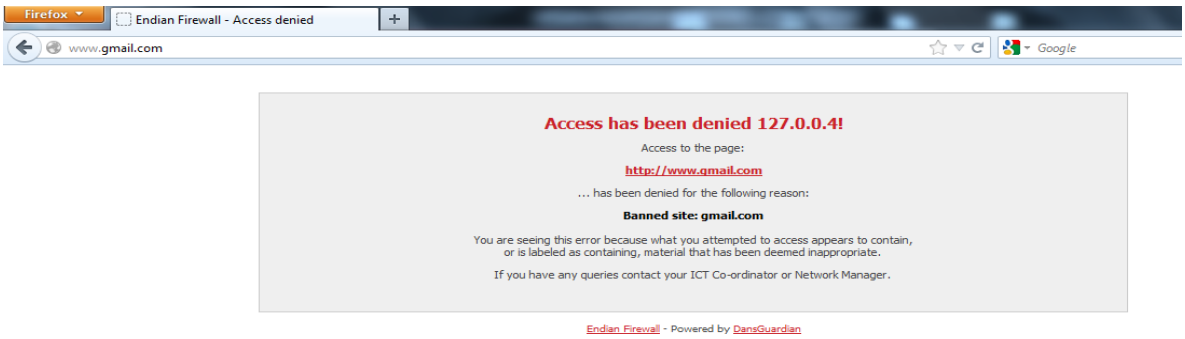


Imagen n°129 autoría propia del sistema endian firewall

Contenido Adulto

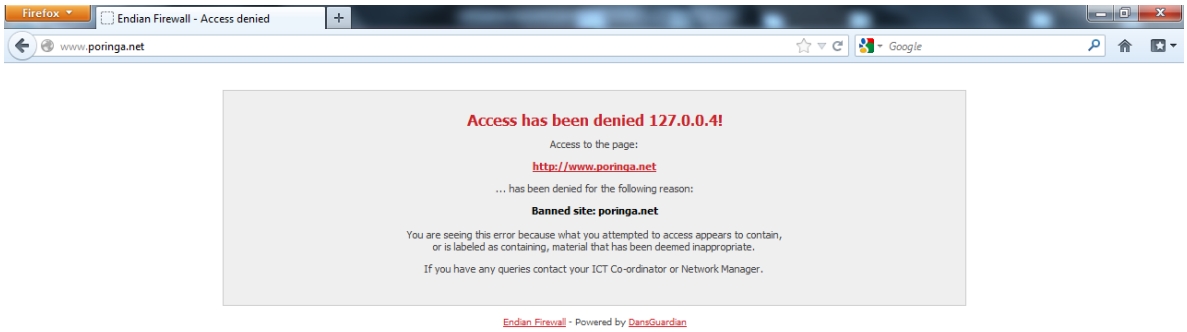


Imagen n°130 autoría propia del sistema endian firewall

Contenido (Chat)

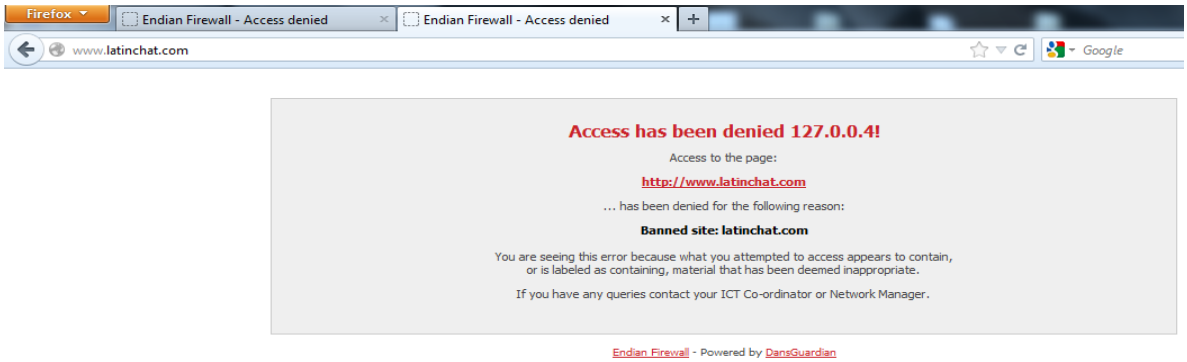


Imagen n°131 autoría propia del sistema endian firewall

Contenido Entretenimiento

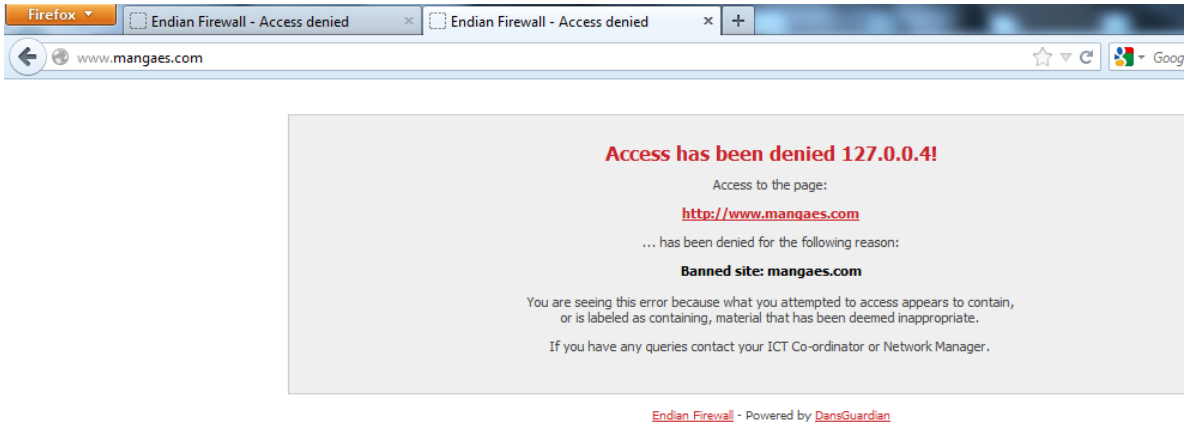


Imagen n°132 autoría propia del sistema endian firewall

Esta acciones de denegar, se aplica al todo el contenido seleccionado por el administrador de la red, tales áreas dentro de la empresa, no poseen ningún medio de acceso a internet.

CIERTO ACCESO DETERMINADO *(Ver Anexo 4.6)*

Este proceso, también maneja contenidos de los cuales, se limita a acceder, mediante contenidos de listas por categoría.

Se define, páginas que es autorizado por el administrador de la red, estas páginas que maneja las áreas específicamente de contabilidad, tienen ingreso a webs como url de Bancos, del Sri, de seguro Social entre otras:

Área Contabilidad
Área Auxiliar Contabilidad
Área Producción

Imagen n°133 Contenido de filtro, acceso a cierto contenido

A diferencia del otro tipo de filtro, que bloque todo contenido, este medio de acceso, referente a el acceso a de determinado contenido de información, se establece el acceso a las denominadas listas negras y blancas personalizadas.

En cuanto a los filtros:

- Filtros de páginas que contienen frases de las siguientes categorías. (Filtrado de contenidos)
- Páginas de filtros de contenido de las siguientes categorías URL

La configuración va hacer aplicado de la misma manera que la de bloquear el acceso total, pero la diferencia esta, en habilitar, determinadas páginas webs en los filtros de acceso, mediante:

Imagen n°134 Acceso y bloqueo de páginas web

Todo el contenido que hare referencia a, permitir los siguientes sitios, da el acceso de internet a los usuarios determinados de la empresa, y en la parte izquierda, medios de bloque, destaca todo el contenido que será bloqueado.

Resultado Saliente:

Google.com

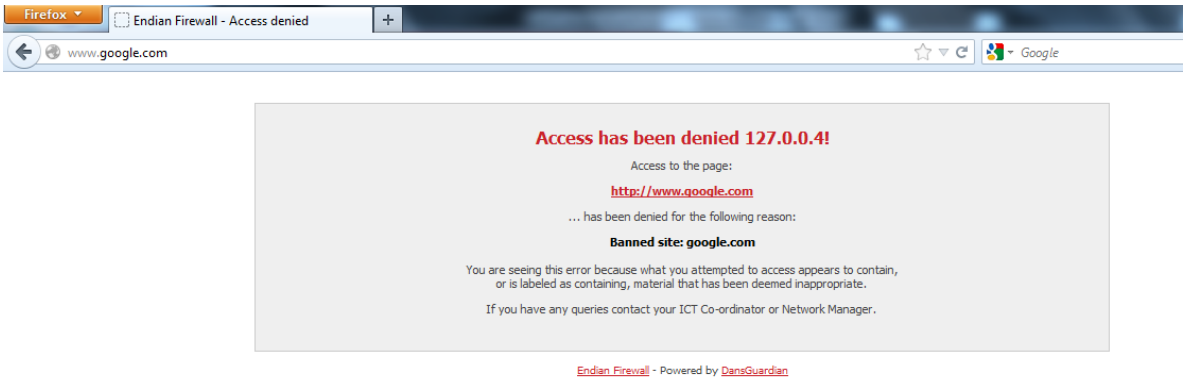


Imagen n°135 autoría propia del sistema endian firewall

Email.

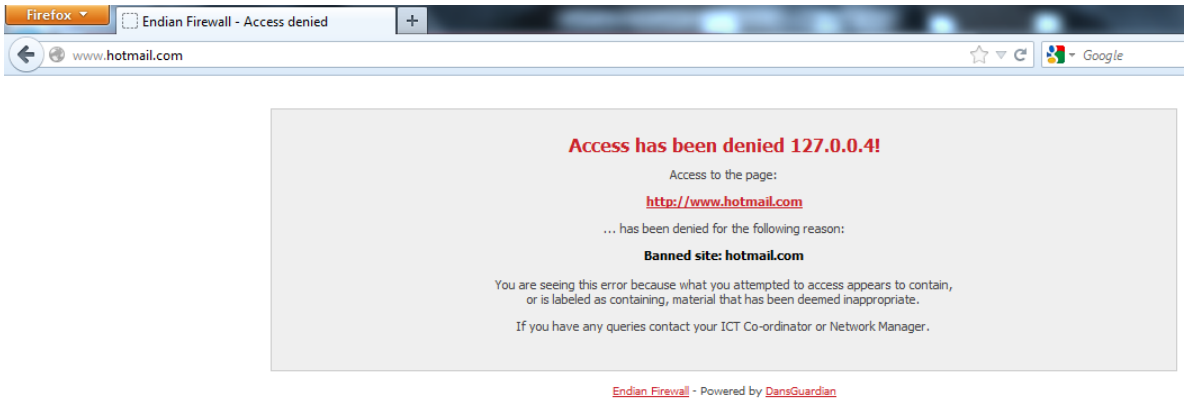


Imagen n°136 autoría propia del sistema endian firewall

Gmail

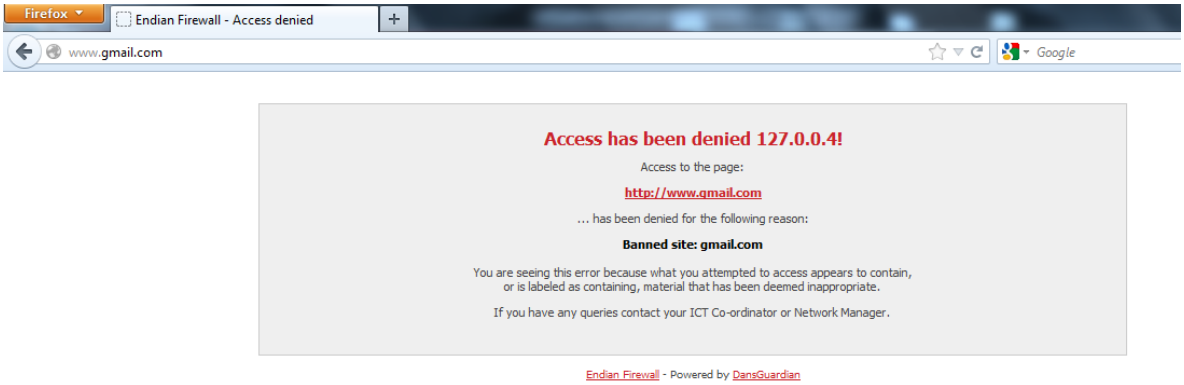


Imagen n°137 autoría propia del sistema endian firewall

Contenido Adulto

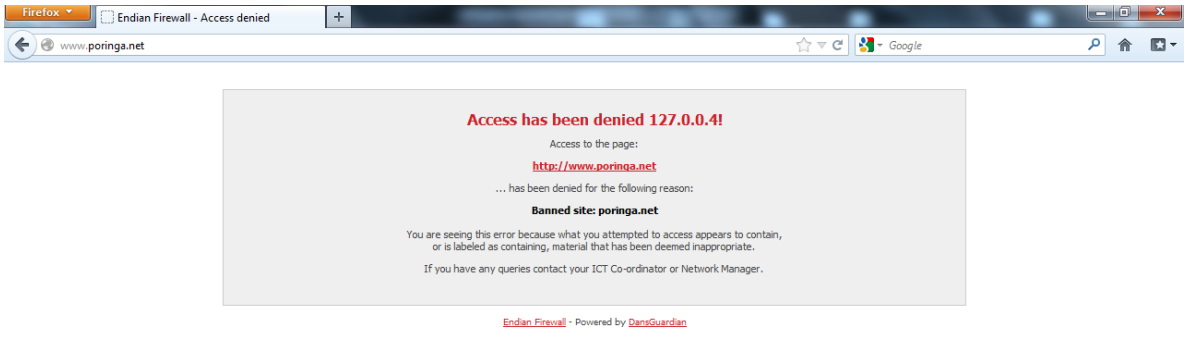


Imagen n°138 autoría propia del sistema endian firewall

Contenido (Chat)

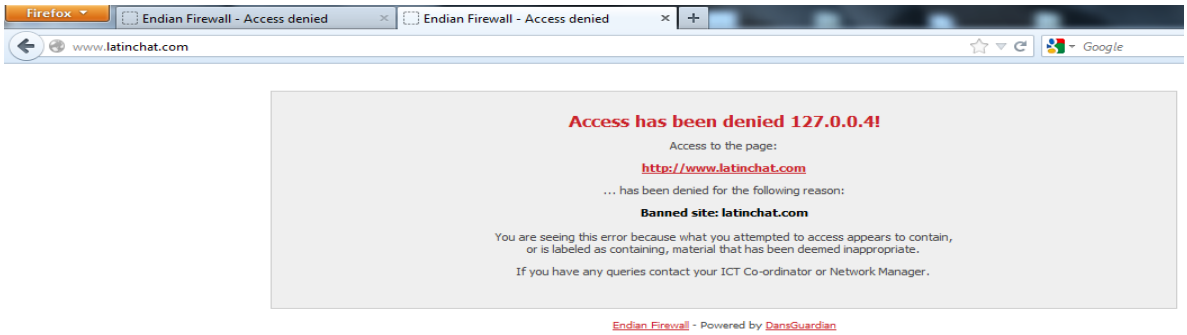


Imagen n°139 autoría propia del sistema endian firewall

Contenido Entretenimiento

Imagen n°140 autoría propia del sistema endian firewall

CIERTO ACCESO DETERMINADO

Contenido SRI

Imagen n°141 SRI

Contenido Bancos

Imagen n°142 página del banco del pichincha

Contenido Iess

Imagen n°143 página del iess

Es decir, esta segmentación de áreas en la red de la empresa, tiene cierto acceso y no acceso a internet.

ACCESO TOTAL A CONTENIDO DE INFORMACION *(Ver Anexo 4.7)*

Aplicado a las siguientes áreas de la Empresa:

Área Administrativa
Área Jefe Personal

Tales áreas, dentro de la empresa, representa altos mandos, en el cual, mencionadas áreas tienen acceso a toda información en la web.

En cuanto a los filtros:

- Filtros de páginas que contienen frases de las siguientes categorías. (Filtrado de contenidos)
- Páginas de filtros de contenido de las siguientes categorías URL
- Listas blancas y negras personalizadas.

Estos filtros, involucran procesos de configuración predeterminada, es decir, no se bloquea, ni se registra procesos de acceso mediante:

Imagen n°144 Filtro de contenido, acceso total

Resultado Saliente:

Google.com

Imagen n°145 autoría propia del sistema endian firewall

Hotmail.com

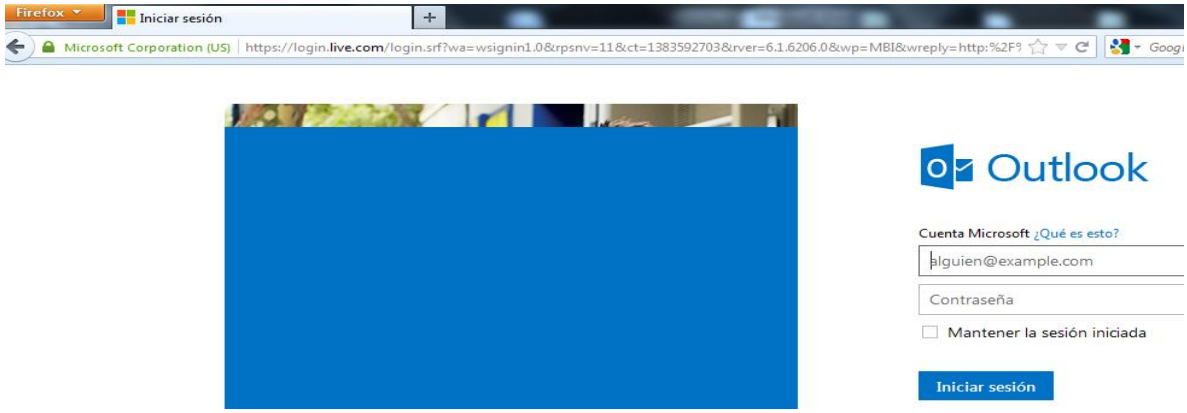


Imagen n°146 autoría propia del sistema endian firewall

Facebook.com

Imagen n°147 autoría propia del sistema endian firewall

Chat.com

Imagen n°148 autoría propia del sistema endian firewall

Es decir, tales áreas dentro de la empresa, poseen cualquier medio de información en el acceso a internet.

4.- Política de Acceso *(Ver Anexo 4.8)*

En esta parte, es establece afinidad con las políticas, es decir, se cruza la política de seguridad con los filtros de acceso:

#	Política	Origen	Destino	Grupo de autor/-usuario	Cuando	Agente de usuario	Actions
1	filter using 'content7'	CUALQUIERA	CUALQUIERA	p1	Siempre	CUALQUIERA	
2	filter using 'content6'	CUALQUIERA	CUALQUIERA	aadministrativa ajefepersonal	Siempre	CUALQUIERA	
3	filter using 'content4'	CUALQUIERA	CUALQUIERA	acompras asecretaria aventas atecnica abodega	Siempre	CUALQUIERA	
4	filter using 'content5'	CUALQUIERA	CUALQUIERA	aproduccion acontabilidad auxconta	Siempre	CUALQUIERA	

Imagen n°149 Cuadro general política de acceso

Filtros en relación a la Segmentación

Filtro 4:

Acceso Total Restringido:

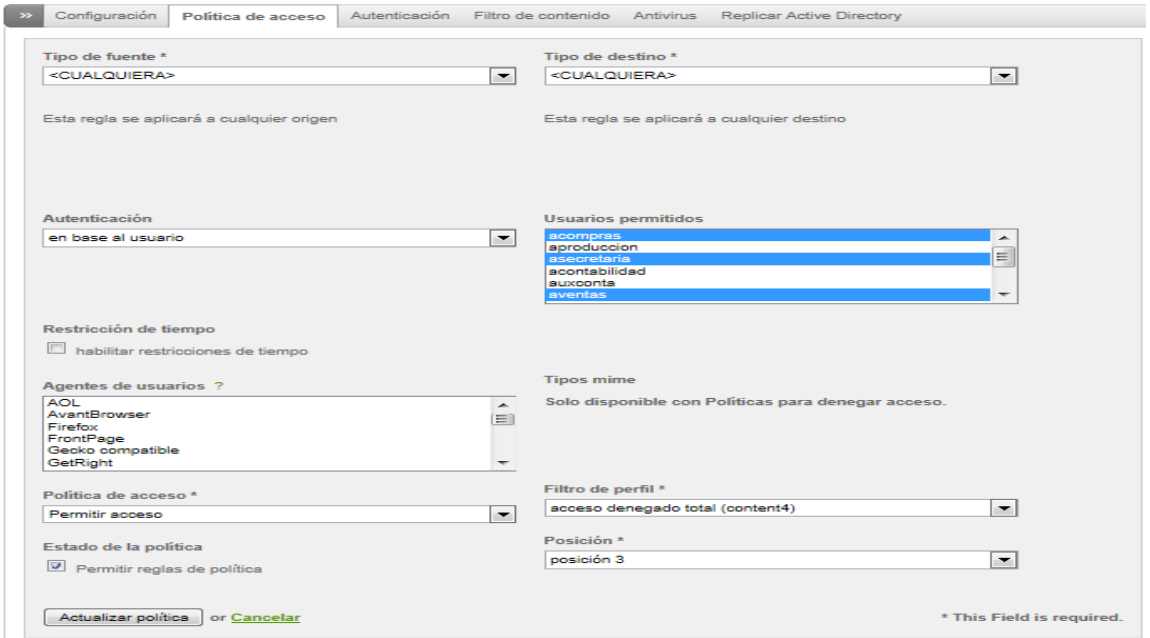


Imagen n°150 Política de acceso, acceso denegado

En esta sección, se ejemplifica la política de seguridad otorgada, en donde, se identifica, el modo de autenticación en base a los usuarios como:

Área Compras
Área Secretaria
Área Ventas
Área Técnica y Tecnológica
Área de Bodega

En la política de acceso, se establece, permitir acceso, pero con el filtro se identifica como acceso denegado total.

Filtro 5:

Acceso a Determinado Contenido:

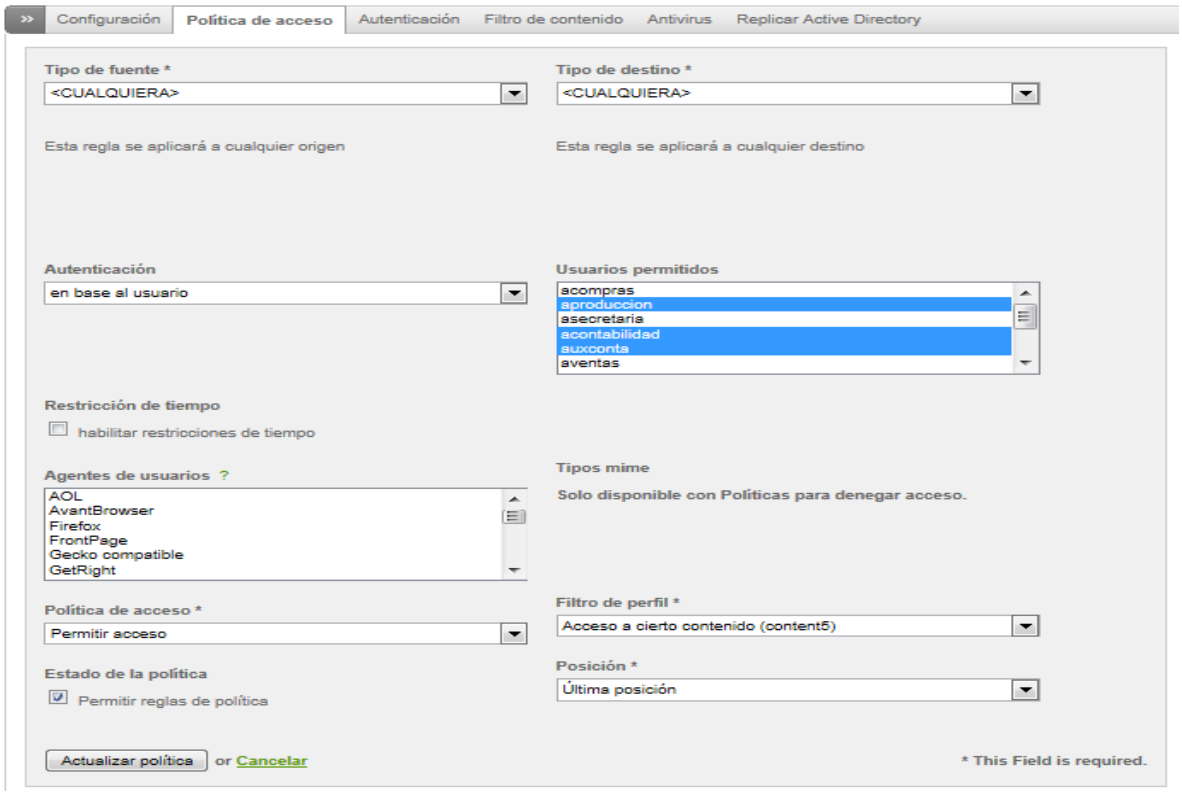


Imagen n°151 Política de acceso, determinado contenido

En esta sección, se ejemplifica la política de seguridad otorgada, en donde, se identifica, el modo de autenticación en base a los usuarios como:

Área Contabilidad
Área Auxiliar Contabilidad
Área Producción

En la política de acceso, se establece, permitir acceso, pero con el filtro se identifica como acceso a cierto contenido.

Filtro 6:

Acceso Total:

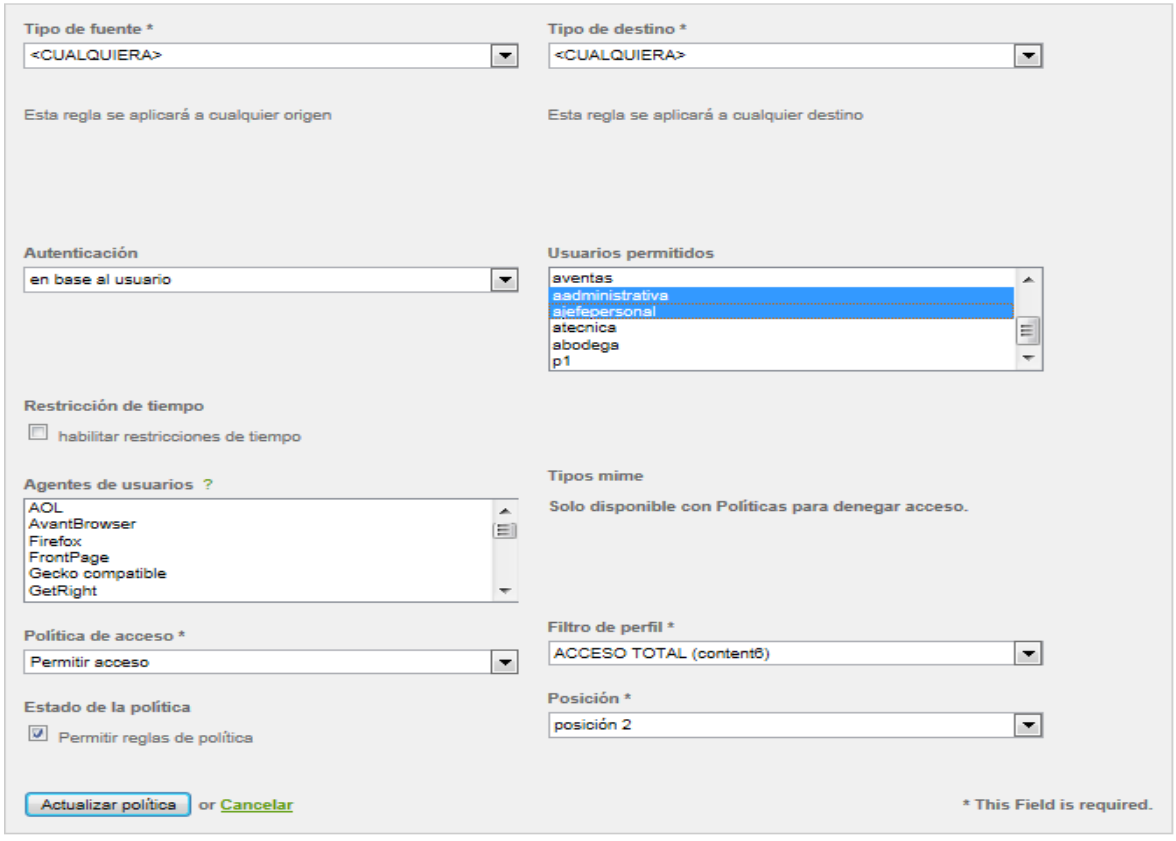


Imagen n°152 Política de acceso, acceso total

En esta sección, se ejemplifica la política de seguridad otorgada, en donde, se identifica, el modo de autenticación en base a los usuarios como:

Área Administrativa
Área Jefe Personal

En la política de acceso, se establece, permitir acceso, pero con el filtro se identifica como ACCESO TOTAL.

DIAGNOSTICAR EL TRÁFICO EN LA RED MEDIANTE EL SISTEMA ENDIAN FIREWALL

DIAGNOSTICAR EL TRÁFICO ENTRANTE Y SALIENTE *(Ver Anexo 5.1)*

Prever el volumen de tráfico de la red es difícil: las tendencias de utilización se basan en crear políticas de seguridad, un aspecto que se verá más adelante.

Imagen n°153: Estatus del sistema

El siguiente paso, es irse a Servicios y activar el tráfico Monitorizado, basado en:

Imagen n°154: Habilitar analizar tráfico

Esta parte es importante proporcionar o habilitar la monitorización del estado actual de la red, mediante el tráfico entrante y saliente.

COMANDOS DE UTILIZACION MODO CONSOLA

- **Levantamiento de servicios, ejecución restauración**

```
[efw-1381796220]: login
root's password:
User root logged in on efw-1381796220.localdomain at 00:32 on 2013-12-19
Welcome to Endian Firewall Community release 2.5.1
Last logged in at 00:30 on 2013-12-19
[efw-1381796220] root: _
```

Imagen n°155: autoría propia del sistema endian firewall

Pasos:

- Ingresar root
- Login
- Job
- Messages

```
[efw-1381796220] root: job
[efw-1381796220] job> messages
```

Imagen n°156: autoría propia del sistema endian firewall

```
2013-12-19 00:08:16 SETXTACCESS-I-Start
2013-12-19 00:09:11 DNSMASQ-I-Restart
2013-12-19 00:09:16 UPLINKSDAEMONJOB-I-Online
2013-12-19 00:09:17 SETPOLICYROUTING-I-Restart
2013-12-19 00:09:17 SETROUTING-I-Restart
2013-12-19 00:09:17 SETSNAT-I-Restart
2013-12-19 00:09:17 DNSMASQ-I-Restart
2013-12-19 00:09:17 IPSEC-I-Restart
2013-12-19 00:09:22 SETINTERFACEMARK-I-Restart
2013-12-19 00:09:24 SETPOLICYROUTING-I-Restart
2013-12-19 00:09:25 SETSNAT-I-Restart
2013-12-19 00:09:34 NTP-I-Restart
2013-12-19 00:09:37 DNSMASQ-I-Restart
2013-12-19 00:09:41 SETXTACCESS-I-Restart
2013-12-19 00:09:42 SETDNAT-I-Restart
2013-12-19 00:09:42 SETINCOMING-I-Restart
2013-12-19 00:09:47 SETOUTGOING-I-Restart
2013-12-19 00:09:48 SETPOLICYROUTING-I-Restart
2013-12-19 00:09:48 SETVPNFW-I-Restart
2013-12-19 00:09:52 SETXTACCESS-I-Restart
2013-12-19 00:09:52 QOS-I-Restart
2013-12-19 00:11:02 SSH-I-Restart
2013-12-19 00:11:11 SETXTACCESS-I-Restart
2013-12-19 00:11:20 SSH-I-Restart
[efw-13817962220] job> _
```

Imagen n°157: autoría propia del sistema endian firewall

Todos los servicios en habilitados y reiniciándose.

- **Levantamiento de servicios, ejecución restauración**

Servidor, Sistema de Seguridad Endian Firwall, servidor propio de la empresa.

```
Available global commands:

exit                          Exit from the current command.
help                          Help command.
logout                        Logout the interactive shell.
[efw-1382380736] show network> summary
Interface    Zone          Address/Mask       Broadcast       MAC Address
br0          GREEN      192.168.0.15/24   192.168.0.255 00:0c:29:c6:bf:48
br1          ORANGE        10.0.0.1/24      10.0.0.255 00:0c:29:c6:bf:52
br2          -                           -            - e6:a7:7f:0d:36:83
eth0         GREEN                       -            - 00:0c:29:c6:bf:48
eth1         ORANGE                      -            - 00:0c:29:c6:bf:52
eth2         -       192.168.159.150/24 192.168.159.255 00:0c:29:c6:bf:5c
lo           -              127.0.0.1/8 127.255.255.255 00:00:00:00:00:00
[efw-1382380736] show network> _
```

Imagen n°158: autoría propia del sistema endian firewall

- **Cambio de contraseña root, administrador**

```
2) Change Root Password
3) Change Admin Password
```

Imagen n°159: autoría propia del sistema endian firewall

```
Choice: 2
Enter Root Password: _
```

Imagen n°160: autoría propia del sistema endian firewall

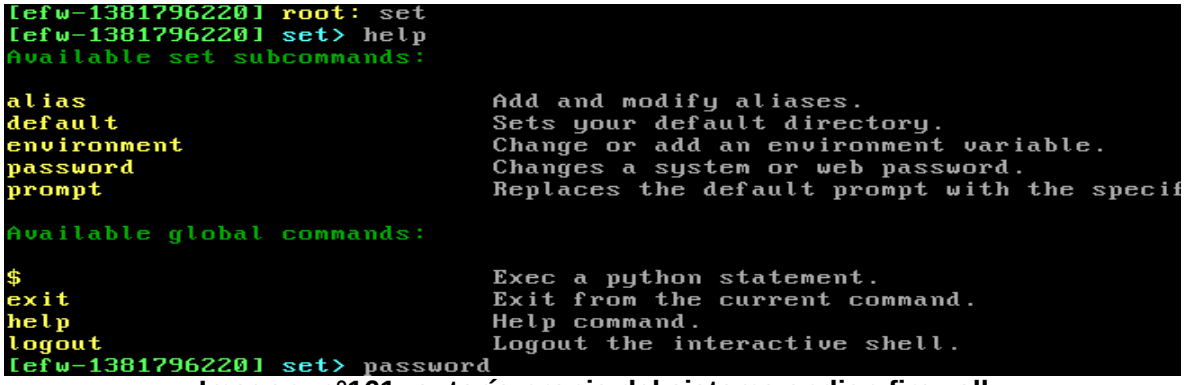


Imagen n°161: autoría propia del sistema endian firewall

- **Servicios modo ayuda**

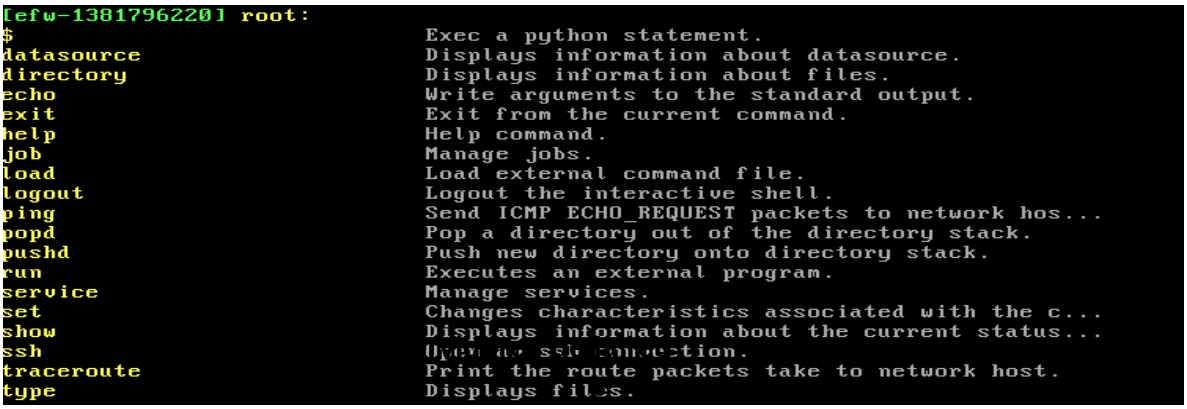


Imagen n°162: autoría propia del sistema endian firewall

Pasos:

- Ingresar root
- Login
- show
- Network
- Address

```
[efw-13817962220] show network> address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 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 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN qlen 1000
    link/ether 00:0c:29:72:6b:27 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN qlen 1000
    link/ether 00:0c:29:72:6b:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.254/24 brd 192.168.0.255 scope global eth1
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN qlen 1000
    link/ether 00:0c:29:72:6b:3b brd ff:ff:ff:ff:ff:ff
5: br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether da:61:96:02:f2:7a brd ff:ff:ff:ff:ff:ff
6: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether c2:f4:ed:c8:aa:a4 brd ff:ff:ff:ff:ff:ff
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:0c:29:72:6b:27 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.15/24 brd 192.168.0.255 scope global br0
[efw-13817962220] show network>
```

Imagen n°163: autoría propia del sistema endian firewall

- **Memoria especificada del Endian Firewall**

Pasos:

- Ingresar root
- Login
- show
- memory

```
MemTotal:        2074848 kB      MemFree:         1538660 kB
Buffers:           39544 kB      Cached:           147964 kB
SwapCached:            0 kB      Active:           408732 kB
Inactive:          85680 kB      Active(anon):     306920 kB
Inactive(anon):       92 kB      Active(file):     101812 kB
Inactive(file):    85588 kB      Unevictable:           0 kB
Mlocked:               0 kB      HighTotal:       1191880 kB
HighFree:         732344 kB      LowTotal:         882968 kB
LowFree:          806316 kB      SwapTotal:        524280 kB
SwapFree:         524280 kB      Dirty:               256 kB
Writeback:             0 kB      AnonPages:        306860 kB
Mapped:            15816 kB      Shmem:               108 kB
Slab:              32264 kB      SReclaimable:      16364 kB
SUnreclaim:        15900 kB      KernelStack:        1680 kB
PageTables:         2212 kB      NFS_Unstable:          0 kB
Bounce:                0 kB      WritebackTmp:          0 kB
CommitLimit:     1561704 kB      Committed_AS:     829980 kB
VmallocTotal:     122880 kB      VmallocUsed:        6512 kB
VmallocChunk:      81820 kB      HardwareCorrupted:     0 kB
HugePages_Total:       0        HugePages_Free:        0
HugePages_Rsvd:        0        HugePages_Surp:        0
Hugepagesize:       4096 kB      DirectMap4k:        8184 kB
DirectMap4M:      897024 kB

[efw-13817962220] show>
```

Imagen n°164: autoría propia del sistema endian firewall

- **Version Endial Firewall Kernel**

Pasos:

  - Ingresar root
  - Login
  - show
  - status

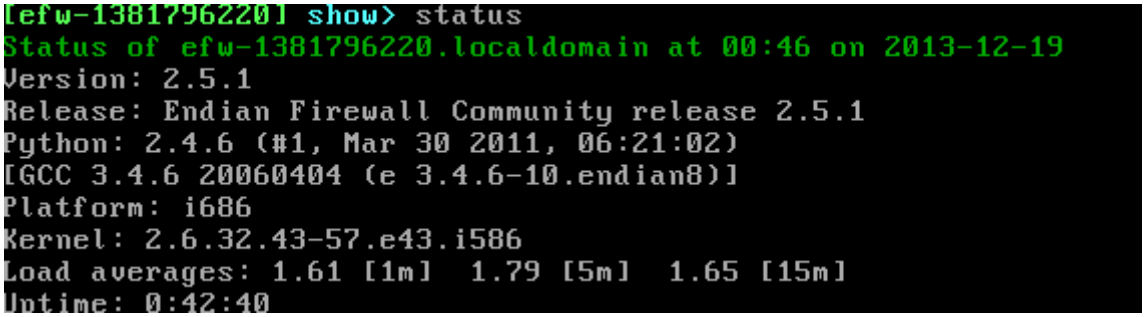


Imagen n°165: autoría propia del sistema endian firewall

- **Lenguaje modo filtros de configuración proxy**

  ln -s /usr/share/dansguardian/languages/mxspanish /usr/share/dansguardian/languages/es

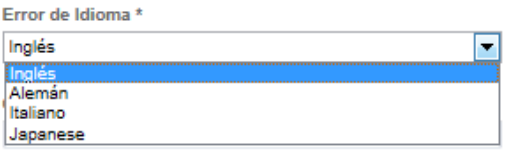


Imagen n°166: autoría propia del sistema endian firewall

- **Copia de Respaldo (Backup)**

Imagen n°167: autoría propia del sistema endian firewall

- **Levantamiento de todos los servicios:**

Snort

```
2013-12-19 01:02:18 SNORTRULES-I-Restart                                0  102
```

Servicios Generales

```
[efw-1381796220] root: sudo /etc/init.d/havp stopt
Usage: /etc/init.d/havp {start|stop|restart|reload|condrestart|condstop|status}
[efw-1381796220] root: sudo /etc/init.d/havp stop
Shutting down HTTP virus scanner (havp):                   [  OK  ]
[efw-1381796220] root: sudo /etc/init.d/havp stop_
```

Imagen n°168: autoría propia del sistema endian firewall

Ejecución

```
[efw-1381796220] root: sudo /etc/init.d/havp start
Starting HTTP virus scanner (havp):                        [  OK  ]
```

Imagen n°169: autoría propia del sistema endian firewall

El modulo se encuentra activado

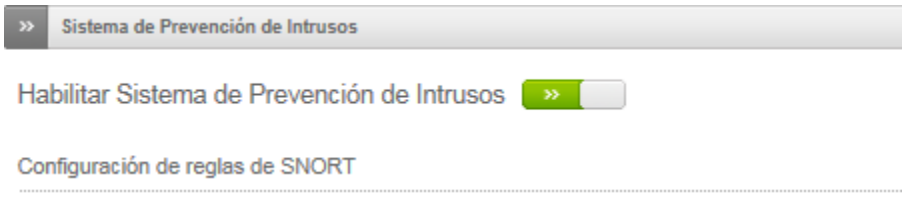


Imagen n°170: autoría propia del sistema endian firewall

Clamav Antivirus

Servicios Generales

```
[efw-1381796220] root: sudo /etc/init.d/havp status
havp (pid 13107 13106 13105 13104 13102 13101 13099 13098 13097 13096 13095 1309
4 13093 13092 13090 13089 13088 13087 13086 13085 13084 13083 13082 13081 13080
13079 13078 13077 13076 13075 13074 13073 13072 13071 13069 13068 13067 13066 13
065 13064 13062) is running...
```

Imagen n°171: autoría propia del sistema endian firewall

Ejecución

```
[efw-1381796220] root: sudo /etc/init.d/havp  start
Starting HTTP virus scanner (havp):
```

Imagen n°172: autoría propia del sistema endian firewall

Imagen n°173: autoría propia del sistema endian firewall

Trafico red

Servicios Generales

Imagen n°174: autoría propia del sistema endian firewall

Ejecución

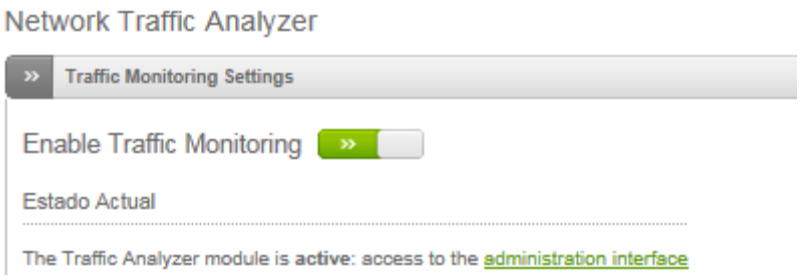
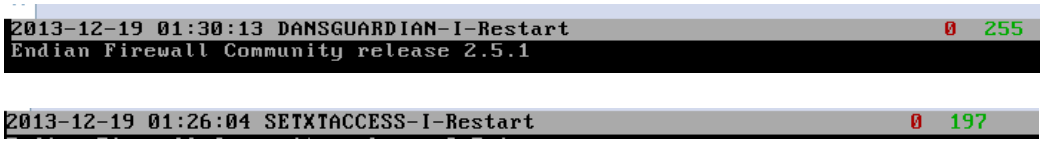


Imagen n°175: autoría propia del sistema endian firewall

Servidor Proxy

Imagen n°176: autoría propia del sistema endian firewall



Servicios Generales

```
[efw-1381796220] root: sudo /etc/init.d/dansguardian  start
Starting dansguardian:
```

Imagen n°177: autoría propia del sistema endian firewall

- Inicio winbind
- Inicio squid
- Inicio DANSGUARDIAN .- Contenido de Filtro
- Inicio SETACCESS.- Políticas de Seguridad

Ejecución

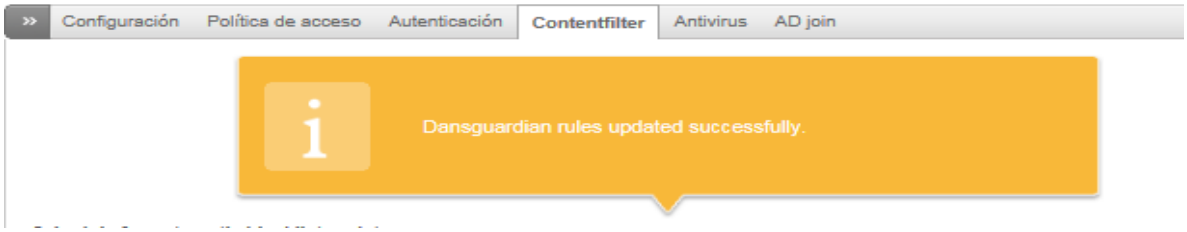


Imagen n°178: autoría propia del sistema endian firewall

#	Política	Origen	Destino	Grupo de autor/-usuario	Cuando	Agente de usuario	Actions
1	filter using 'content6'	CUALQUIERA	CUALQUIERA	aadministrativa ajefepersonal	Siempre	CUALQUIERA	
2	filter using 'content4'	CUALQUIERA	CUALQUIERA	acompras asecretaria aventas atecnica abodega	Siempre	CUALQUIERA	
3	filter using 'content5'	CUALQUIERA	CUALQUIERA	aproduccion acontabilidad auxconta	Siempre	CUALQUIERA	
4	filter using 'content1'	CUALQUIERA	CUALQUIERA	conta	Siempre	CUALQUIERA	
5	filter using 'content2'	CUALQUIERA	CUALQUIERA	no necesario	Siempre	CUALQUIERA	

IMAGEN N°179: AUTORIA PROPIA DEL SISTEMA ENDIAN FIREWALL

REPORTES

Logs Vivos

Filtro de Contenido

Acceso Denegado

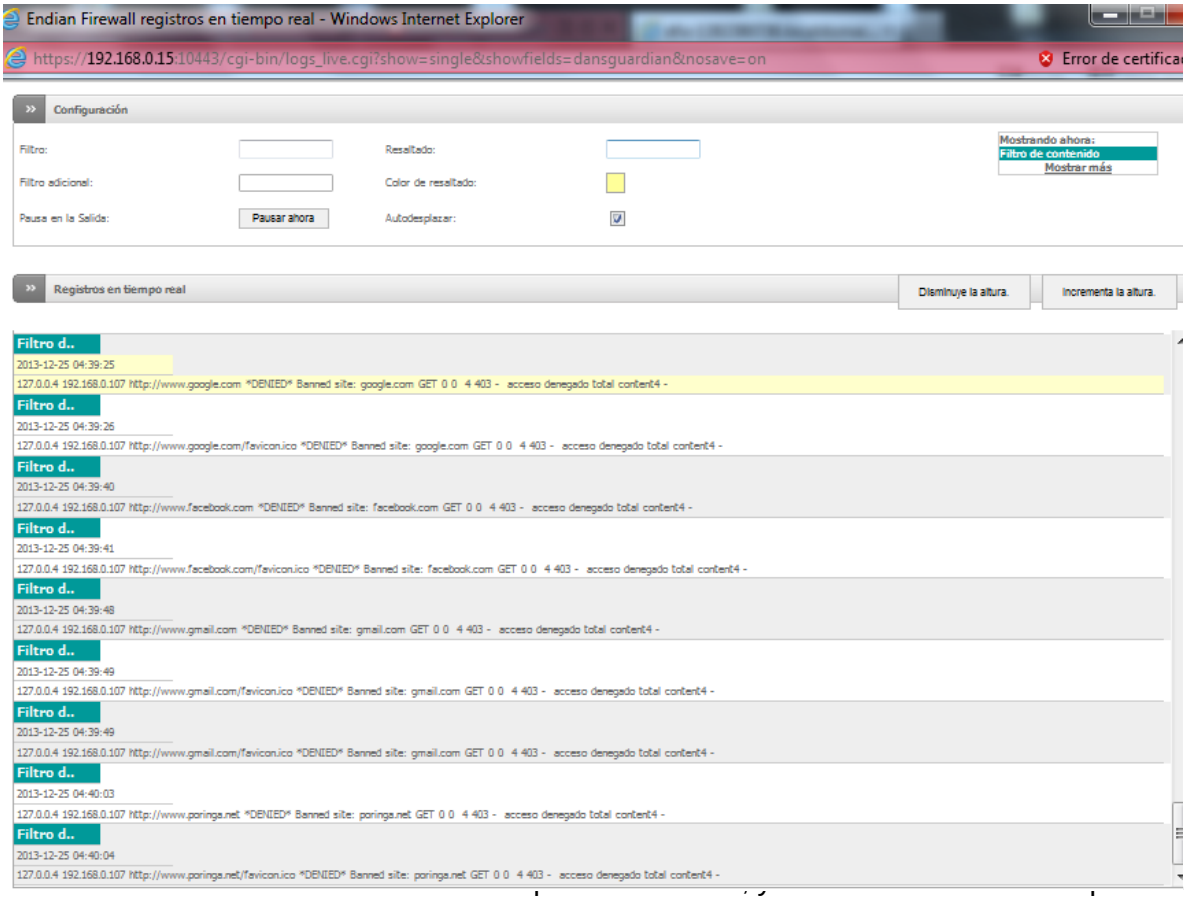


Imagen n°180: autoría propia del sistema endian firewall

Acceso a cierto contenido

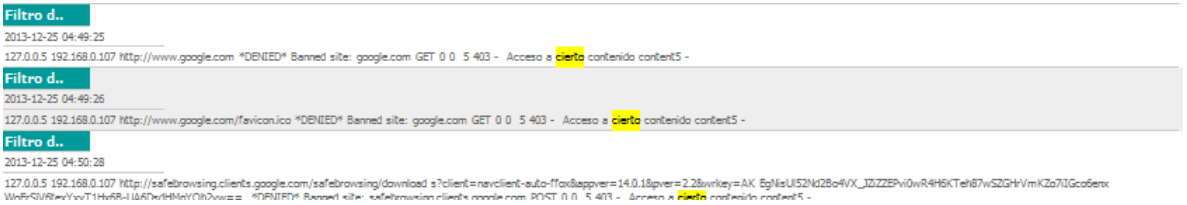


Imagen n°181: autoría propia del sistema endian firewall

Proxy

HTTP

Enfoque de Control

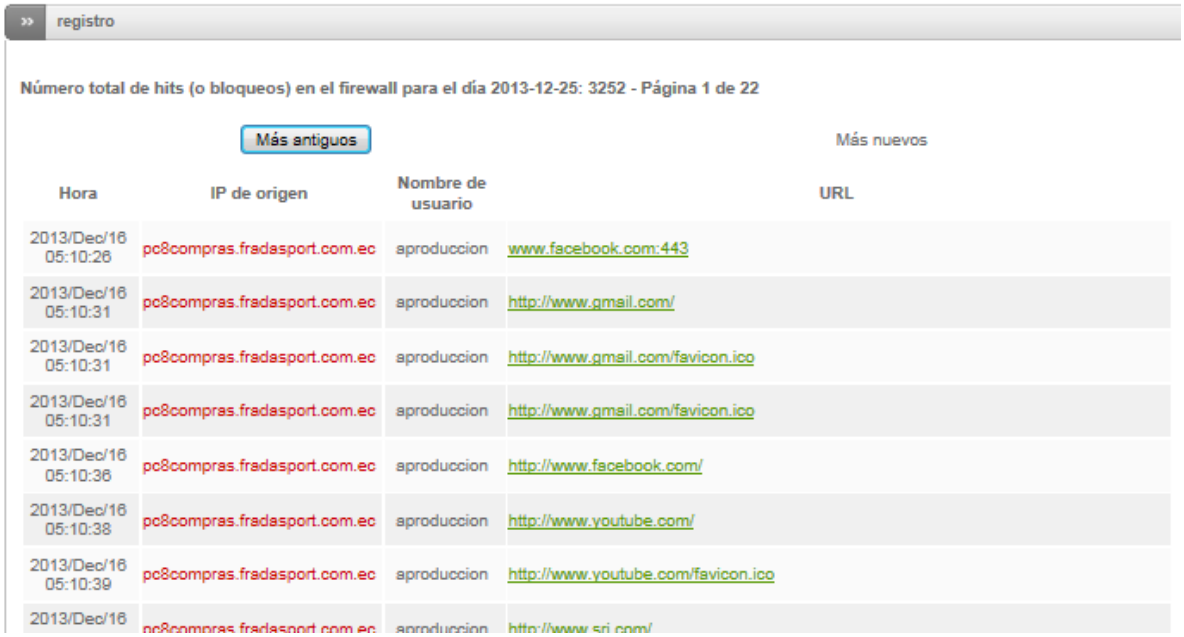


Imagen n°182: autoría propia del sistema endian firewall

El usuario de producción, ingreso a contenido de información, el log de registros, permite enfocar y visualizar todo el contenido de información que todo el personal de la empresa a accedido, como asunto de la correcta administración y control de los usuarios de la empresa.

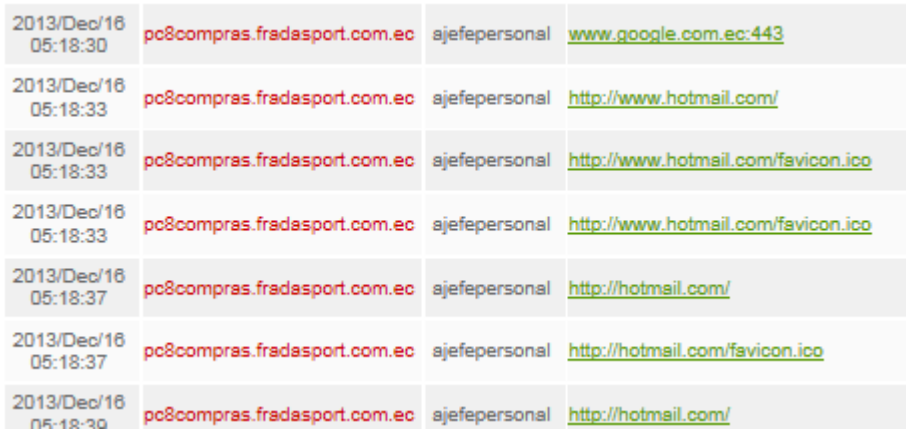


Imagen n°183: autoría propia del sistema endian firewall

Incluye, la fecha, hora, nombre de equipo, numero de pc, y el ingreso url.

Filtro de contenido HTTP

Registros de bloqueo Firewall

Imagen n°184: autoría propia del sistema endian firewall

Se destaca, todo el almacenamiento de información referente al contenido.

2013/Dec/16 05:23:57	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.gmail.com/favicon.ico	DENIED
2013/Dec/16 05:23:58	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.gmail.com/favicon.ico	DENIED
2013/Dec/16 05:24:03	pc8compras.fradasport.com.ec (127.0.0.4)	https://www.facebook.com:443	DENIED
2013/Dec/16 05:24:08	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.facebook.com	DENIED
2013/Dec/16 05:24:18	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.youtube.com	DENIED
2013/Dec/16 05:24:18	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.youtube.com/favicon.ico	DENIED
2013/Dec/16 05:24:26	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.poringa.net	DENIED
2013/Dec/16 05:24:27	pc8compras.fradasport.com.ec (127.0.0.4)	http://www.poringa.net/favicon.ico	DENIED
2013/Dec/16 05:27:03	pc8compras.fradasport.com.ec (127.0.0.4)	http://safebrowsing.clients.google.com/safebrowsing/download...	DENIED

Imagen n°185: autoría propia del sistema endian firewall

Incluye la posibilidad de poder exportar a un archivo txt.

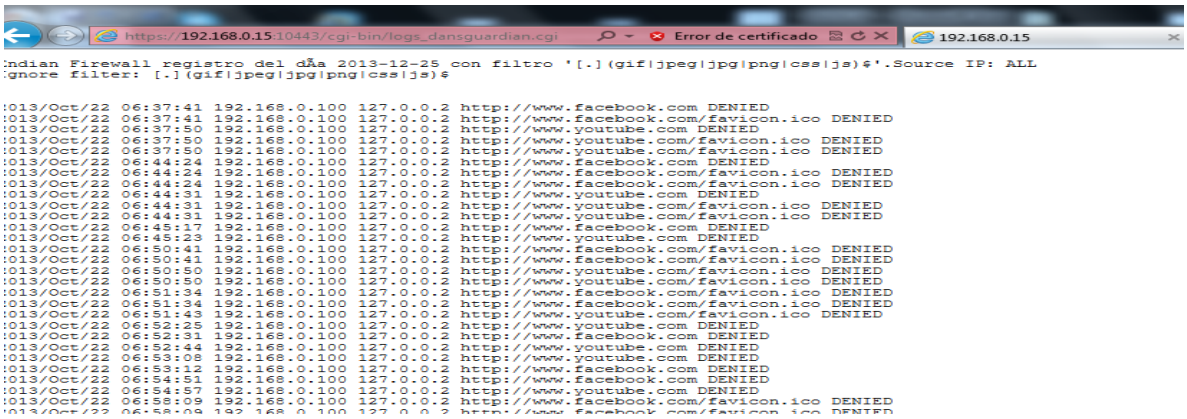


Imagen n°186: autoría propia del sistema endian firewall

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORIZACIÓN DE EMPASTADO

Quito enero07, 2014
OFI-060-AE-UP-14

Señor
JUAN JACOB BUENO ROSALES
ESTUDIANTE DE LA CARRERA DE SISTEMAS INFORMÁTICOS
UNIVERSIDAD TECNOLÓGICA ISRAEL

Presente.-

De mi consideración:

Una vez revisadas las modificaciones de los informes emitidos, autorizamos al estudiante JUAN JACOB BUENO ROSALES, alumno de la CARRERA DE SISTEMAS INFORMÁTICOS, proceda con la impresión y presentación del empastado para el tema de tesis SISTEMA DE CONTROL Y SEGURIDAD ENDIAN FIREWALL PARA LA EMPRESA FRADA SPORT, para que siga con el proceso de graduación y defensa respectiva.

Cordialmente,

Mg. Oswaldo Basurto

MIEMBRO DEL TRIBUNAL

CC. Secretaría Académica