ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación.

Maestría En Seguridad Informática Aplicada.

"DISEÑO E IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PERIMETRAL Y MONITOREO PARA LA RED DE DATOS EN UNA EMPRESA INDUSTRIAL."

EXAMEN DE GRADO (COMPLEXIVO)

PREVIA A LA OBTENCIÓN DEL TITULO DE

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

CHRISTIAN MAURICIO MIRANDA MOREIRA

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

En primer lugar a mi amor por haberme guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de los que son parte de mi familia a mi abuelita Aurora, a mi madre Soledad, mi hermano Javier, mis tías y tíos, mis amigos por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Por último a mis maestros y compañeros de maestría porque en esta armonía grupal hemos alcanzado esta importante meta en nuestra carrera profesional.

Christian Miranda Moreira

DEDICATORIA

Dedico este proyecto de tesis a mi Abuelita Aurora y a mi familia. A mi abuelita porque estuvo conmigo en cada etapa de mi vida, cuidándome y dándome fortaleza para seguir adelante, a mi familia, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ellos que soy lo que soy ahora. Los amo con toda mi vida.

Christian Miranda Moreira

TRIBUNAL DE SUSTENTACIÓN

_____	_____
MGS. Karina Astudillo	**Ing. Juan Carlos García**
PROFESOR DELEGADO	PROFESOR DELEGADO
POR LA SUBDECANA DE LA	POR LA SUBDECANA DE LA
FIEC	FIEC

RESUMEN

Las empresas industriales además de perseguir la eficiencia de sus procesos y alcanzar sus logros económicos a través de la comercialización de sus productos, también tienen su gestión administrativa, en la que se persiguen otros objetivos que van de la mano con los objetivos estratégicos del negocio. Estas organizaciones como cualquier otra necesitan proteger sus activos críticos de cualquier eventualidad que pueda suceder y afecten su funcionamiento. En la empresa industrial donde se desarrolla la solución propuesta en este proyecto de tesis, se consideran como parte de sus activos críticos los sistemas informáticos, no solo porque albergan datos importantes, sino también porque generan información importante del proceso de gestión de producción , comercial y financiera ,ya actualmente no se les da el suficiente resguardo, la presente investigación propone un esquema de seguridad perimetral para la red de datos de esta organización ; además del desarrollo de un esquema de monitoreo proactivo de la seguridad perimetral establecida.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

Direccionamiento IP.- Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI.

Disponibilidad de datos.- El término disponibilidad de datos se refiere a que los datos contenidos al interior de cualquier base de datos este siempre al alcance, cuando se la requiera.

Firewall.- Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Integridad de datos.- El término integridad de datos se refiere a la corrección y complementación de los datos en una base de datos.

Hackers.- Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de

computadoras y de redes informáticas.

HTTP.- Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.

IPS.- Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Norma ISO/IEC 27002.- ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la International Organization for Standardization y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013.

PING.- Como programa, ping es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de

solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

Punto de Red de datos.- Punto físico donde un dispositivo electrónico tendrá acceso a la red interna o externa.

Servidor de correo.- Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Servidor de dominio.- Un Servidor de Nombres de Dominio (DNS) o "servidor de nombres" es un servidor que mapea o conecta un nombre de dominio con una dirección de IP específica. En definitiva indica el dominio (y todo el tráfico del dominio) al que acceder en Internet.

Servidor MPLS.- Servidor donde se hospeda el servicio de automatización de todas las máquinas industriales de la organización.

Servidor BRILL.-Servidor donde se hospeda la aplicación de recetas de producción, previo la ejecución de una orden de fabricación de productos.

Subred.- Las subredes son un método para maximizar el espacio de direcciones IPv4 de 32 bits Además de hacer que el espacio de la dirección IPv4 sea más eficaz, las subredes presentan varias ventajas administrativas y de seguridad.

SSH.- SSH (Secure Shell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TCP.- Transmission Control Protocol (TCP) o Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.1

Url Filtering.- Es un término que describe un software diseñado para restringir o controlar el contenido de un lector está autorizado a acceder, especialmente cuando se utiliza para restringir el material entregado a través de Internet a través de la Web, correo electrónico, o por otros medios.

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El permanente desarrollo tecnológico, el nivel de competencia, la estrategia y el mercado globalizado en las organizaciones hacen que las redes de datos estén inmersas a riesgos inherentes y peligros tales como intentos de accesos foráneos no autorizados, ataques por parte del personal y sobre todo a los externos como hackers con fines malintencionados. Este alto índice de exposición se traduce en amenazas que podrían afectar el nivel de integridad y confiabilidad de las redes de datos en las organizaciones y por consecuencia repercusión en la información financiera de estas.

Como parte del proceso en la cual las Organizaciones deben desarrollarse para asegurar sus redes de datos, surge la seguridad informática como una necesidad con el propósito de proteger su información ante posibles daños a la que puede estar sujeta por acción de cualquier intruso o grupo que desee y pueda tener acceso malintencionado a ella. Estos daños pueden provocar la pérdida total, parcial o la modificación de los datos; Actualmente las empresas son el principal objetivo para realizar todo tipo de ataque informático, ya que para el hacker o hacker resulta atractivo provocar una pérdida económica para su satisfacción o bienestar personal.

La seguridad perimetral es un mecanismo para defender las redes de datos, que consiste en instalar equipos de comunicaciones en los que se establece políticas de seguridad acompañadas de procedimientos necesarios para precautelar su mantenibilidad y óptimo funcionamiento, estos equipos se colocan entre la Red Wan y la red interna, permitiendo o denegando el acceso a usuarios internos y externos a los diferentes recursos de la red.

La implementación de la seguridad perimetral consta de cinco etapas: Análisis a la situación actual de la red, Segmentación de la Red, Segmentación de los servicios de la red, Implementación de políticas en los módulos del Firewall y esquema de monitoreo de la red. Para el diseño del sistema de seguridad perimetral es imprescindible realizar un análisis a la situación actual de la red, logrando así saber cuál de los segmentos de red de datos necesitan más protección, es decir que segmento de red debe tener o no permisos para acceder a determinados servicios de red o internet. Sin embargo, a pesar de que las organizaciones están impulsando proyectos de aseguramiento de las redes de datos, todavía se evidencia que este tipo de esfuerzos son más de carácter reactivo que preventivo, es decir que, se corrige el problema cuando ya este ha ocurrido, por ello, la implementación de un esquema de seguridad perimetral en la red de datos de las organizaciones, en este caso las empresas industriales se considera como un factor crítico para proteger la seguridad de su información.

CAPÍTULO 1

1 GENERALIDADES.

1.1 Descripción del Problema.

Hoy en día la información representa el activo más importante en las organizaciones, independiente cual sea su naturaleza de negocio, por lo tanto se la debe proteger ante riesgos existentes en el entorno, tanto internos como externos. Los riesgos internos son las amenazas propias de la organización o del entorno cercano donde se administra la información, tales como recursos tecnológicos, humanos o procesos , y los riesgos externos son amenazas del entorno exterior, en definitiva, cualquier recurso humano o tecnológico ajeno a la organización que tenga acceso a Internet.

Siempre existirán amenazas latentes en cualquier ámbito, es por eso que la seguridad nunca debe ser poco estimada ya que siempre pueden existir intereses maliciosos para obtener o alterar la información de las organizaciones.

La infraestructura actual de red de la empresa industrial no fue planeada con un enfoque de seguridad ya que se alinea con un esquema tradicional de una red plana, que consiste en mantener la comunicación interna y externa a través de un equipo de comunicación sin capacidad de enrutamiento con un direccionamiento IP para todas las áreas que integran la organización, con puertos abiertos, sin excepción de permisos, y con acceso irrestricto desde y hacia el internet. Existen ciertos puntos de control a través de un proxy server con políticas básicas que han venido creando bajo solicitud de la gerencia general. , pero no valoraciones previas que justifiquen dichos puntos; Sin embargo el crecimiento permanente de la Institución ha llevado a la modificación del esquema de red actual, junto con procesos y procedimientos adecuados que precautelen la integridad y disponibilidad de su información.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCION.

2.1.- Levantamiento de información.

La metodología propuesta para la implementación de la seguridad perimetral consta de 3 etapas claramente identificadas:

- Evaluación de Riesgos
- Arquitectura de la solución
- Esquema de Monitoreo

2.2. Evaluación de riesgos

En la organización no existen servicios muy críticos o información sensible que estén albergados en los sistemas tecnológicos, es por esto que se aplicará el método Baseline Approach para evaluar los riesgos de seguridad a la que una organización está expuesta. Ésta metodología propone prácticas reconocidas para la selección de contramedidas de seguridad que más se adecuen a los sistemas tecnológicos.

El proceso de realizar la evaluación de riesgos se compone de varias etapas:

- Inventario de activos
- Valoración de activos
- Análisis de amenazas
- Análisis de vulnerabilidades
- Análisis de riesgos

2.2.1.- Inventario de activos

Se consideran activos importantes dentro del ámbito tecnológico de la empresa industrial según análisis preliminar los siguientes:

CÓDIGO (AC = ACTIVO)	ACTIVOS IMPORTANTES
AC1	Servidor de Correo
AC2	Servidor de dominio
AC3	Switches de enlace a todos los centros de cómputo de la organización
AC4	Enlace de comunicación WAN

Tabla 2.2.1.-Identificaciòn de activos

2.2.2.- Valoración de activos

Es importante valorar los activos según su importancia en la organización, la valoración se realiza según el impacto negativo que tendría la pérdida, daño o destrucción de dicho activo. (Refiérase a la tabla 2.2.1 para identificar los activos)

CÓDIGO (AC = ACTIVO)	VALORACIÓN
AC1	Alto

AC2	Alto
AC3	Medio
AC4	Alto

Tabla 2.2.2.-Valoración de activos

2.2.3.- Análisis de amenazas

Siempre existen amenazas inherentes donde existe una infraestructura de sistemas tecnológicos, es importante identificar la probabilidad de que éstas ocurran, de qué forma ocurrirían y a que activos afectarían.

La escala a usarse para las causas de las amenazas es A (accidental), M (ambiental), D (deliberado), y ALTA, MEDIA y BAJA.

2.3.3.1 Probabilidad que las amenazas ocurran

PROBABILIDAD QUE LAS AMENAZAS OCURRAN		
AMENAZA	**CAUSA**	**PROBABILIDAD**
Terremoto	M	MEDIA

Inundación	A,M.D	ALTA
Relámpago	M	MEDIA
Bomba	A.D	BAJA
Armas De Fuego	A,D	MEDIA
Fuego	A,M,D	ALTA
Error involuntario	D	ALTA
Falta de suministro eléctrico	A	MEDIA
Error en hardware	A	MEDIA
Variación de Voltaje	A	ALTA
Temperatura elevada	A,M	ALTA
Humedad muy elevada	M	BAJA
Carga electrostática	A,D	MEDIA
Robo	D	MEDIA
Error operativo	A,D	MEDIA
Error por mantenimiento	A,D	MEDIA

Fallas de Software	A,D	MEDIA
Software mal usado	A,D	MEDIA
Software instalado sin autorización	D	ALTA
Suplantación de Identidad	D	ALTA
Malware	D	ALTA
Acceso no autorizado a la red	D	ALTA
Exceso de tráfico	A,D	MEDIA
Fallo de Componentes en la red	A	ALTA
Recursos mal utilizados	A,D	MEDIA
Personal insuficiente	A	BAJA

Tabla 2.2.3.1.- Probabilidad y Causa de explotación de amenazas

2.3.3.2 Activos afectados por explotación de amenazas

Estos serían los activos afectados en el supuesto caso de que una amenaza se convierta en un hecho real:

PROBABILIDAD DE EXPLOTACIÓN DE AMENAZAS	
ACTIVOS AFECTADOS POR EXPLOTACIÒN DE AMENAZAS	
AMENAZA	**ACTIVOS AFECTADOS**
Terremoto	Servidores , Switches, Router
Inundación	Todos
Relámpago	Servidores , Switches, Router
Bomba	Todos
Armas de fuego	Todos
Fuego	Servidores , Switches, Router
Error involuntario	Todos
Falta de suministro eléctrico	Servidores , Switches, Router
Error en hardware	Todos

Variación de Voltaje	Servidores , Switches, Router
Temperatura elevada	Servidores , Switches, Router
Humedad muy elevada	Servidores , Switches, Router
Carga Electroestática	Servidores , Switches, Router
Robo	Todos
Error operativo	Servidores , Switches, Router
Error por mantenimiento	Servidores , Switches, Router
Fallas de Software	Servidores , Switches, Router
Software mal usado	Servidores , Switches, Router

Tabla 2.2.3.2.- Activos afectados por explotación de amenazas

2.2.4.- Análisis de vulnerabilidades

Existen acciones de toda clase que pueden explotar ciertas vulnerabilidades, en diferentes ámbitos:

2.2.4.1 Ambiente e infraestructura

AMBIENTE E INFRAESTRUCTURA	
VULNERABILIDAD	**ACCIÓN QUE LA EXPLOTARÍA**
Falta de protección física de las puertas en los centros de cómputo	Robo
Control de acceso insuficiente en la organización	Error involuntario, Robo
Área propensa a inundación	Inundación
Falta de detectores de humo	Fuego
Falta de sistema de control de temperatura	Temperatura elevada
Susceptibilidad al polvo	Polvo
Susceptibilidad a los ataques internos	Software instalado sin autorización

Tabla 2.2.4.1.- Ambiente e infraestructura

2.2.4.2 Hardware

HARDWARE	
VULNERABILIDAD	**ACCIÓN QUE LA EXPLOTARÍA**
Fallos de hardware por variación de temperatura	Temperatura elevada
Fallos de hardware por voltaje inestable	Variaciones de voltaje
Susceptibilidad a la radiación electromagnética	Manejo erróneo al instalar componentes de hardware

Tabla 2.2.4.2.- Hardware

2.2.4.3 Comunicaciones

COMUNICACIONES	
VULNERABILIDAD	**ACCIÓN QUE LA EXPLOTARÍA**
Falta de autenticación en la red	Acceso no autorizado a la red

Transferencia de contraseñas	Suplantación de Identidad
Inadecuada administración de la red	Exceso de tráfico

Tabla 2.2.4.3.-Comunicaciones

2.2.4.4 Personal

PERSONAL	
VULNERABILIDAD	**ACCIÓN QUE LA EXPLOTARÍA**
Ausencia de personal	Personal insuficiente
Trabajo de terceros no supervisado	Robo
Entrenamiento de seguridad insuficiente	Error operativo
Uso incorrecto de hardware y software	Error operativo, Recursos mal utilizados

Tabla 2.2.4.4.- Personal

2.2.5.- Análisis de riesgos

2.2.5.1 Servidor de Correo

SERVIDOR DE CORREO				
Amenaza	**Valor de activo (A)**	**Probab. Ocurrencia (B)**	**Riesgo (A x B)**	**Ranking**
Temperatura elevada	5	5	25	1
Error involuntario	5	4	20	2
Variación de Voltaje	5	4	20	3
Suplantación de Identidad	5	4	20	4
Software Malicioso	5	4	20	5
Falta de suministro eléctrico	4	4	16	6
Error en hardware	4	4	16	7
Software instalado sin autorización	5	3	15	8
Acceso no autorizado a la red	5	3	15	9
Exceso de tráfico	5	3	15	10

Robo	4	3	12	11
Fallo de Componentes en la red	3	4	12	12
Inundación	5	2	10	13
Fuego	5	2	10	14
Humedad muy elevada	5	2	10	15
Fallas de Software	5	2	10	16
Error operativo	4	2	8	17
Error por mantenimiento	4	2	8	18
Software mal usado	4	2	8	19
Mal uso de recursos	3	2	6	20
Terremoto	5	1	5	21
Bomba	5	1	5	22
Relámpago	3	1	3	23
Armas de Fuego	3	1	3	24
Carga Electroestática	3	1	3	25

Tabla 2.2.5.1.-Servidor de correo

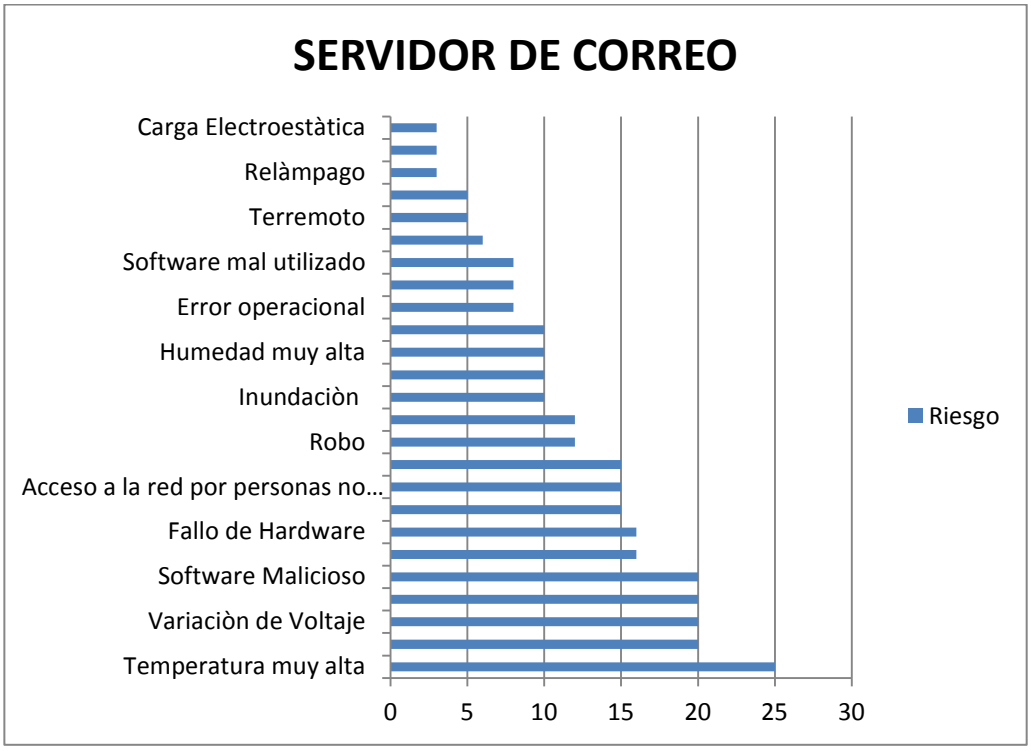

Figura 2.2.5.1.-Servidor de Correo

2.2.5.2 Servidor de dominio

SERVIDOR DE DOMINIO				
Amenaza	**Valor de activo (A)**	**Probab. Ocurrencia (B)**	**Riesgo (A x B)**	**Ranking**
Temperatura elevada	5	5	25	1
Suplantación de Identidad	5	5	25	2

Error involuntario	5	4	20	3
Software Malicioso	5	4	20	4
Software instalado sin autorización	5	4	20	5
Acceso no autorizado a la red	5	4	20	6
Falta de suministro eléctrico	4	4	16	7
Variación de Voltaje	5	3	15	8
Error en hardware	4	3	12	9
Robo	4	3	12	10
Error operativo	4	3	12	11
Error por mantenimiento	4	3	12	12
Inundación	5	2	10	13
Fuego	5	2	10	14
Relámpago	5	2	10	15
Exceso de tráfico	3	3	9	16
Fallas de Software	4	2	8	17

Software mal usado	4	2	8	18
Mal uso de recursos	4	2	8	19
Armas de Fuego	4	2	8	20
Carga Electroestática	4	2	8	21
Fallo de Componentes en la red	3	2	6	22
Humedad muy elevada	5	1	5	23
Terremoto	5	1	5	24
Bomba	5	1	5	25

Tabla 2.2.5.2.- Servidor de dominio

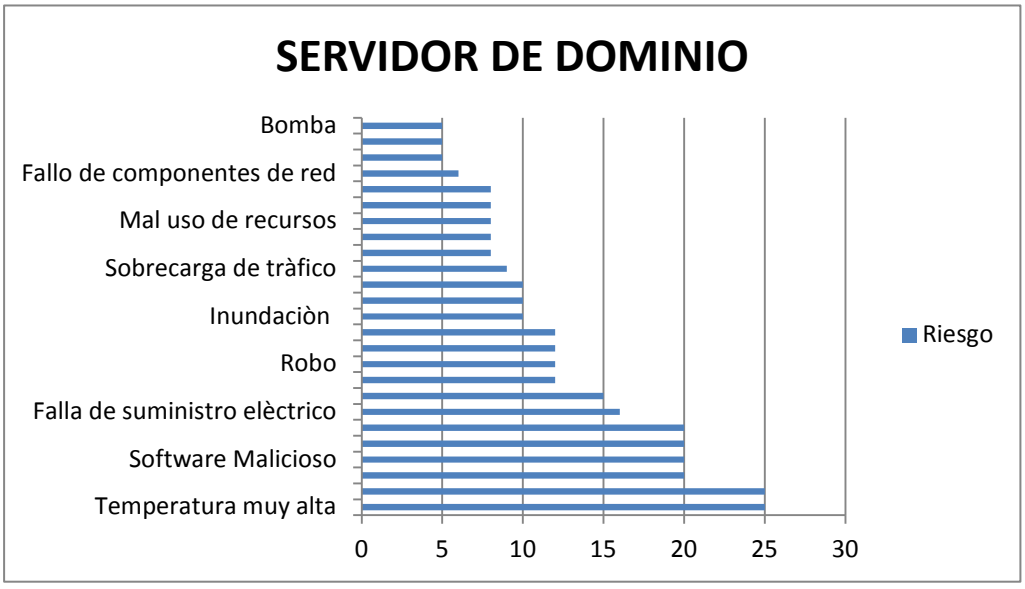

Figura 2.2.5.2.- Servidor de dominio

2.2.5.3 Enlaces de comunicación

ENLACES DE COMUNICACIÓN A CENTROS DE DISTRIBUCIÒN				
Amenaza	**Valor de activo (A)**	**Probab. Ocurrencia (B)**	**Riesgo (A x B)**	**Ranking**
Temperatura elevada	5	5	25	1
Variación de Voltaje	4	4	16	2
Robo	5	3	15	3
Inundación	5	3	15	4
Carga Electroestática	4	3	12	5
Error involuntario	5	2	10	6
Error en hardware	5	2	10	7
Fuego	5	2	10	8
Relámpago	5	2	10	9
Fallo de Componentes en la red	5	2	10	10
Mal uso de recursos	3	3	9	11

Falta de suministro eléctrico.	4	2	8	12
Error operativo	4	2	8	13
Error por mantenimiento	3	2	6	14
Exceso de tráfico	2	3	6	15
Armas de Fuego	5	1	5	16
Terremoto	5	1	5	17
Bomba	5	1	5	18
Software Malicioso	1	4	4	19
Acceso no autorizado a la red.	1	4	4	20
Suplantación de Identidad	1	3	3	21
Software instalado sin autorización.	1	3	3	22
Fallas de Software	1	3	3	23
Software mal usado	1	2	2	24
Humedad muy elevada	1	1	1	25

Tabla 2.2.5.3.-Enlaces de comunicación

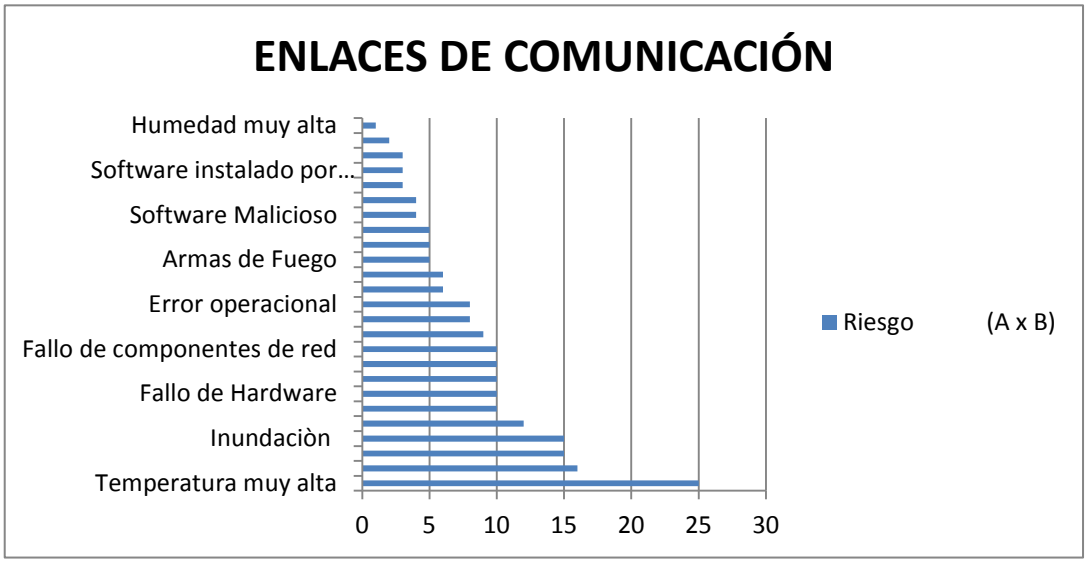

Figura 2.2.5.3.-Enlaces de comunicación

2.2.5.4 Servidor de producción MPLS

SERVIDOR DE PRODUCCION MPLS				
Amenaza	**Valor de activo (A)**	**Probab. Ocurrencia (B)**	**Riesgo (A x B)**	**Ranking**
Temperatura elevada	5	5	25	1
Variación de Voltaje	4	4	16	2
Robo	5	3	15	3
Inundación	5	3	15	4

Carga Electroestática	4	3	12	5
Error involuntario	5	2	10	6
Error en hardware	5	2	10	7
Fuego	5	2	10	8
Relámpago	5	2	10	9
Fallo de Componentes en la red	5	2	10	10
Mal uso de recursos	3	3	9	11
Falta de suministro eléctrico.	4	2	8	12
Error operativo	4	2	8	13
Error por mantenimiento	3	2	6	14
Sobrecarga de tráfico	2	3	6	15
Armas de Fuego	5	1	5	16
Terremoto	5	1	5	17
Bomba	5	1	5	18

Software Malicioso	1	4	4	19
Acceso no autorizado a la red.	1	4	4	20
Suplantación de Identidad	1	3	3	21
Software instalado sin autorización.	1	3	3	22
Fallas de Software	1	3	3	23
Software mal usado	1	2	2	24
Humedad muy elevada	1	1	1	25

Tabla 2.2.5.4.- Servidor de producción MPLS

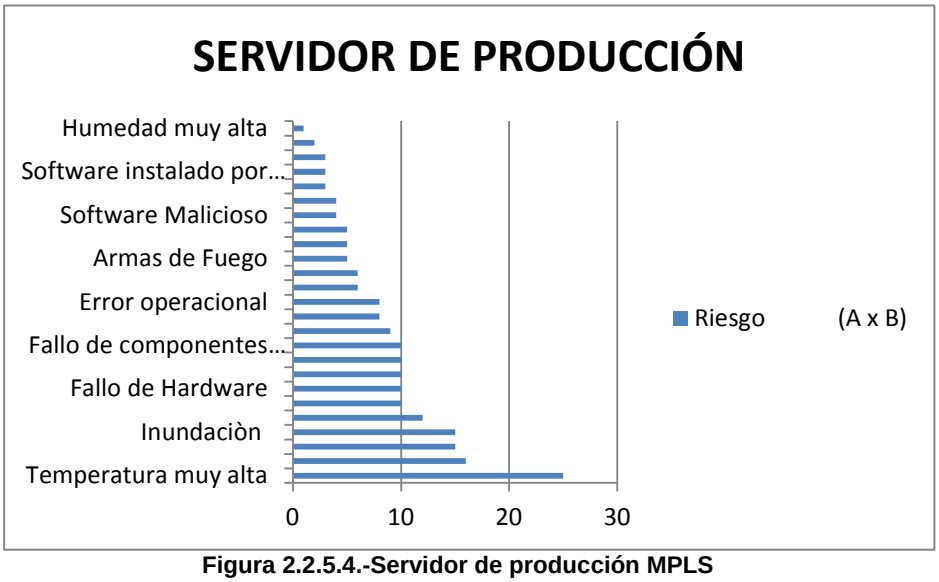

Figura 2.2.5.4.-Servidor de producción MPLS

2.2.5.5 Servidor de Control de Calidad BRILL

SERVIDOR DE CONTROL DE CALIDAD BRILL				
Amenaza	**Valor de activo (A)**	**Probab. Ocurrencia (B)**	**Riesgo (A x B)**	**Ranking**
Variación de Voltaje	5	3	15	5
Error involuntario	5	2	10	6
Software instalado sin autorización.	5	3	15	6
Fallo de Componentes en la red	5	3	15	7
Error en hardware	4	3	12	8
Robo	5	2	10	9
Mal uso de recursos	5	2	10	10
Falta de suministro eléctrico.	5	2	10	11
Error operativo	4	2	8	12
Error por	4	2	8	13

mantenimiento				
Relámpago	4	2	8	14
Carga Electroestática	4	2	8	15
Fallas de Software	4	2	8	16
Software mal usado	4	2	8	17
Exceso de tráfico	3	2	6	18
Fuego	5	1	5	19
Inundación	5	1	5	20
Terremoto	5	1	5	21
Bomba	5	1	5	22
Armas de Fuego	5	1	5	23
Temperatura elevada	2	1	2	24
Humedad muy elevada	1	1	1	25

Tabla 2.2.5.5.-Servidor de Control de Calidad BRILL

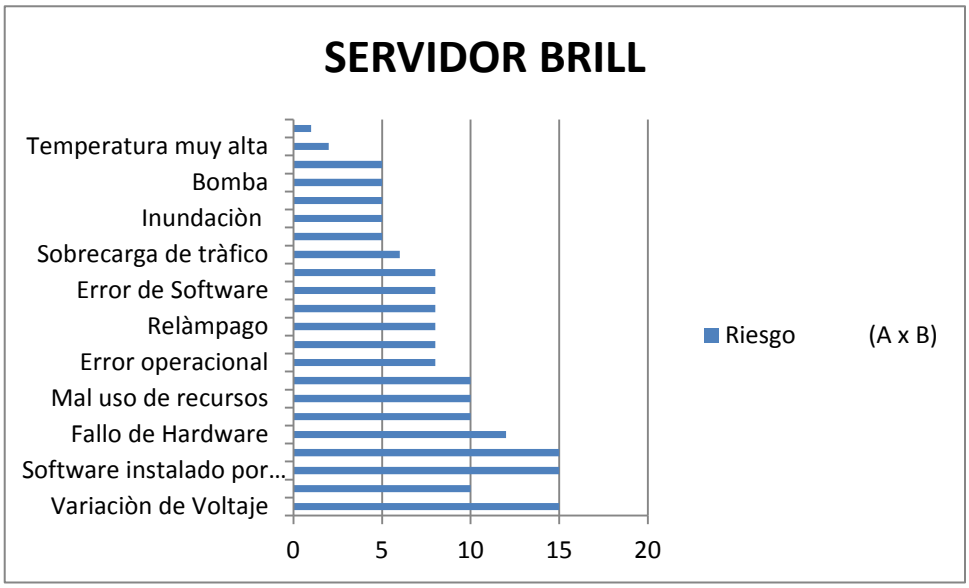

Figura 2.2.5.5.-Servidor de control de calidad BRILL

2.3 Arquitectura de la solución

Con el propósito de iniciar un proceso de implementación del Sistema de Gestión de Seguridad de la Información en la organización se han desarrollado contramedidas basadas en la norma ISO/IEC 27002 que a más de incrementar el nivel de seguridad lógica, física, Organizacional, legal, y de crear un marco de seguridad informática con un manual de políticas del área de tecnología y un plan de contingencia ante desastres, es importante también crear un esquema de seguridad perimetral eficiente que ayude a minimizar el riesgo inherente que los activos informáticos presentan y complemente el marco de seguridad informática que se desea establecer.

El esquema de seguridad perimetral propuesto es el siguiente:

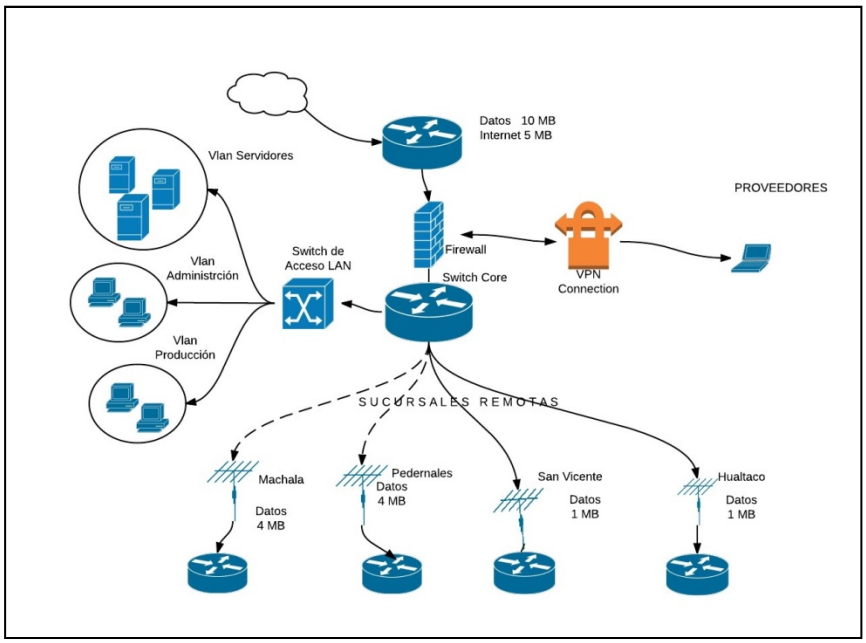

Figura 2.3.-Arquitectura de la solución

Este esquema permite incrementar el nivel de seguridad perimetral reorganizando los componentes críticos de la red y aumentando otros, basándose en una estructura de seguridad perimetral definida.

La estructura consiste en añadir 1 firewall en donde se realizará las configuraciones correspondientes para poder diferenciar 3 segmentos de red:

- Red Wan
- Red desmilitarizada (DMZ)
- Red Lan

De ésta manera aumenta el nivel de seguridad en la red, ya que en un supuesto caso de un ataque, tendrán que ser comprometido el firewall para poder ingresar a la Red Lan.

2.3.1.- Red Wan

La Red Wan es el Internet, donde no hay ningún tipo de restricción de tráfico ni garantiza ningún nivel de seguridad, aquí se va a exponer el módulo IPS del Firewall.

2.3.2.- Red desmilitarizada (DMZ)

La Red desmilitarizada o DMZ es un segmento de red donde se ubican los servidores que tengan que recibir cierto tipo de tráfico entrante desde la Red Wan, por ejemplo, servidores proxy, de correo, filtros de contenido, ftp, servidores web, etc., es decir, es un segmento con un nivel de seguridad medio ya que permite el ingreso de ciertos paquetes filtrados por el firewall externo. Para las necesidades de la red de la empresa industrial, es necesario realizar las configuraciones en el módulo URL FILTERING e IPS para que controlen el tráfico de este segmento en particular.

2.3.3.- Red Lan

La Red Lan tiene un nivel alto de seguridad y confiabilidad, ya que la mayor parte del tráfico es saliente y el tráfico entrante es muy limitado y proviene solo de los servidores de la Red desmilitarizada (DMZ) que ya ha sido filtrado por el firewall externo y adicionalmente serán filtrados por el firewall interno.

2.3.3.1 Distribución de puntos de Red

Para realizar la segmentación de la red, es necesario que se encuentren documentados todos los puntos finales de los usuarios con su correspondiente puerto en los equipos de comunicación.

USUARIO	DPTO.	Piso / Planta	RACK	SWITCH	PUERTOS	VLAN
aadams	cartera	Alta	R1	A	9	Vlan _Administracion
vacio	cartera	Alta	R1	A	11	Vlan _Administracion
vacio	cartera	Alta	R1	A	12	Vlan _Administracion
vacio	cartera	Alta	R1	A	13	Vlan _Administracion
vacio	cartera	Alta	R1	A	14	Vlan _Administracion
vacio	cartera	Alta	R1	A	15	Vlan _Administracion
vacio	cartera	Alta	R1	A	16	Vlan _Administracion
vacio	ventas	Alta	R1	A	17	Vlan _Administracion
vacio	ventas	Alta	R1	A	18	Vlan

						_Administracion
ogutierrez	ventas	Alta	R1	A	19	Vlan _Administracion
vacio	ventas	Alta	R1	A	20	Vlan _Administracion
vacio	ventas	Alta	R1	A	21	Vlan _Administracion
vacio	ventas	Alta	R1	A	22	Vlan _Administracion
mencalada	ventas	Alta	R1	A	23	Vlan _Administracion
vacio	ventas	Alta	R1	A	24	Vlan _Administracion
vacio	ventas	Alta	R1	B	1	Vlan _Administracion
vacio	ventas	Alta	R1	B	2	Vlan _Administracion
vacio	ventas	Alta	R1	B	3	Vlan _Administracion

vacio	ventas	Alta	R1	B	4	Vlan _Administracion
vacio	ventas	Alta	R1	B	5	Vlan _Administracion
vacio	ventas	Alta	R1	B	6	Vlan _Administracion
vacio	ventas	Alta	R1	B	7	Vlan _Administracion
vacio	ventas	Alta	R1	B	8	Vlan _Administracion
vacio	ventas	Alta	R1	B	9	Vlan _Administracion
vacio	ventas	Alta	R1	B	10	Vlan _Administracion
vacio	ventas	Alta	R1	B	11	Vlan _Administracion
vacio	ventas	Alta	R1	B	12	Vlan _Administracion
copiadora	ventas	Alta	R1	B	13	Vlan

						_Administracion
vacio	ventas	Alta	R1	B	14	Vlan _Administracion
vacio	contabilidad	Baja	R1	B	15	Vlan _Administracion
vacio	contabilidad	Baja	R1	B	16	Vlan _Administracion
vacio	contabilidad	Baja	R1	B	17	Vlan _Administracion
vacio	contabilidad	Baja	R1	B	18	Vlan _Administracion
jibarra	contabilidad	Baja	R1	B	19	Vlan _Administracion
jibarra	contabilidad	Baja	R1	B	20	Vlan _administración
jleon	contabilidad	Baja	R1	C	1	Vlan _administración
mpelaez	contabilidad	Baja	R1	C	3	Vlan _administración

acastaneda	caja	Baja	R1	C	5	Vlan _Administracion
copiadora	contabilidad	Baja	R1	C	21	vlan_administracion
vacio	contabilidad	Baja	R1	C	22	vlan_administracion
smedina	contabilidad	Baja	R1	C	23	vlan_administracion
vacio	contabilidad	Baja	R1	C	24	vlan_administracion
jaristega	contabilidad	Baja	R1	D	1	vlan_administracion
vacio	contabilidad	Baja	R1	D	2	vlan_administracion
atorres	cartera	Alta	R1	D	3	vlan_administracion
vacio	ventas	Alta	R1	D	5	vlan_administracion
vacio	ventas	Alta	R1	D	6	vlan_administraci

						on
vacio	recepción	Baja	R1	D	9	vlan_administracion
vacio	recepción	Baja	R1	D	10	vlan_administracion
ggarcia	RRHH	Baja	R2	G	6	vlan_administracion
ggarcia	RRHH	Baja	R2	G	2	vlan_administracion
DVR Administrativo	Cámaras		R2	F	14	vlan_camaras
dsvelez	gerencia	Alta	R1	A	1	Vlan_Gerencia
dsvelez	gerencia	Alta	R1	A	2	Vlan_Gerencia
rbolona	gerencia	Alta	R1	A	3	Vlan_Gerencia
rbolona	gerencia	Alta	R1	A	4	Vlan_Gerencia
rbolona	gerencia	Alta	R1	A	5	Vlan_Gerencia
dsvelez	gerencia	Alta	R1	A	6	Vlan_Gerencia

mbanchon	gerencia	Alta	R1	A	7	Vlan_Gerencia
mbanchon	gerencia	Alta	R1	A	8	Vlan_Gerencia
vacio	presidencia	Baja	R1	C	7	vlan_gerencia
vacio	presidencia	Baja	R1	C	8	vlan_gerencia
vacio	presidencia	Baja	R1	C	9	vlan_gerencia
vacio	presidencia	Baja	R1	C	11	vlan_gerencia
vacio	presidencia	Baja	R1	C	12	vlan_gerencia
vacio	presidencia	Baja	R1	C	13	vlan_gerencia
vacio	presidencia	Baja	R1	C	14	vlan_gerencia
vacio	presidencia	Baja	R1	C	15	vlan_gerencia
vacio	presidencia	Baja	R1	C	16	vlan_gerencia
vacio	presidencia	Baja	R1	C	17	vlan_gerencia
vacio	presidencia	Baja	R1	C	18	vlan_gerencia
vacio	presidencia	Baja	R1	C	19	vlan_gerencia
vacio	presidencia	Baja	R1	C	20	vlan_gerencia
vacio	presidencia	Baja	R1	D	13	vlan_gerencia

vacio	presidencia	Baja	R1	D	14	vlan_gerencia
vacio	presidencia	Baja	R1	D	15	vlan_gerencia
vacio	presidencia	Baja	R1	D	16	vlan_gerencia
jibarra	Nutricion	Alta	R2	G	16	vlan_laboratorio
fgonzalez	Producción	Alta	R2	G	17	vlan_laboratorio
njara	Calidad	Alta	R2	G	18	vlan_laboratorio
iaguirre	Mantenimiento	Bodega Repuestos	R2	G	19	vlan_laboratorio
jibarra	Nutricion	Alta	R2	G	8	vlan_laboratorio
njara	Calidad	Alta	R2	G	10	vlan_laboratorio
PC WinCC	Producción	Cabina de Control	R2	G	1	vlan_produccion
Backup WinCC	Producción	Cabina de Control	R2	G	2	vlan_produccion
Dispositivo	Producción	Cabina	R2	G	4	vlan_produccion

		de Control				
Supervisores	Producción	Baja	R2	G	5	vlan_produccion
vacio	Producción	Baja	R2	G	7	vlan_produccion
jdavila	Mantenimiento	Baja	R2	G	8	vlan_produccion
rordonez	Mantenimiento	Baja	R2	G	9	vlan_produccion
vacio	Producción	Baja	R2	G	10	vlan_produccion
vacio	Producción	Baja	R2	G	11	vlan_produccion
copiadora producción	Producción	Alta	R2	G	12	vlan_produccion
vacio	Producción	Alta	R2	G	13	vlan_produccion
vacio	Producción	Alta	R2	G	14	vlan_produccion
morellana	Mantenimiento	Alta	R2	G	15	vlan_produccion
Supervisor	Producción	Baja	R2	G	1	vlan_produccion

es						
vacio	Producción	Baja	R2	G	3	vlan_produccion
jdavila	Mantenimiento	Baja	R2	G	4	vlan_produccion
rordonez	Mantenimiento	Baja	R2	G	5	vlan_produccion
vacio	Producción	Alta	R2	G	6	vlan_produccion
morellana	Mantenimiento	Alta	R2	G	7	vlan_produccion
fgonzalez	Producción	Alta	R2	G	9	vlan_produccion
Servidor Desarrollo	sistemas		R1	E	22	vlan_servidores
Puerto R1-E3	Sistemas	Baja	R2	F	1	vlan_servidores
Servidor SRVVMWARE	Sistemas	Baja	R2	F	3	vlan_servidores
Servidor SRVVMWA	Sistemas	Baja	R2	F	5	vlan_servidores

RE						
Servidor FILESRV	Sistemas	Baja	R2	F	6	vlan_servidores
ILO SRVVMWARE	Sistemas	Baja	R2	F	7	vlan_servidores
ILO DBAPLICATIVO2	Sistemas	Baja	R2	F	11	vlan_servidores
DBAPLICATIVO2	Sistemas	Baja	R2	F	12	vlan_servidores
jsolano	sistemas	Baja	R1	D	17	vlan_sistemas
jsolano	sistemas	Baja	R1	D	18	vlan_sistemas
vacio	sistemas	Baja	R1	D	19	vlan_sistemas
vacio	sistemas	Baja	R1	D	20	vlan_sistemas
gblanco	sistemas	Baja	R1	D	21	vlan_sistemas
abarona	sistemas	Baja	R1	D	23	vlan_sistemas
vacio	sistemas	Baja	R1	E	1	vlan_sistemas

vacio	sistemas	Baja	R1	E	2	vlan_sistemas
Switch HP (F)	Datacenter	Baja	R1	E	3	
Router Telconet	Datacenter	Baja	R2	F	4	
Router CNT Cisco	Datacenter	Baja	R2	F	15	

Tabla 2.3.3.1.- Distribución de puntos de Red

2.3.4.-Segmentación de la Red

Con el propósito de establecer políticas de seguridad y precautelar la confidencialidad de los datos en la red interna estará segmentada en subredes de la siguiente manera:

VLAN	SEGMENTO DE RED
Vlan Servidores	192.168.10.0/24
Grupo administración	
Vlan Administración	192.168.11.0/24
Wifi_Administracion	192.168.19.0/24
Vlan VoIP	192.168.12.0/24
Vlan Invitados	192.168.13.0/24
Vlan Impresoras	192.168.14.0/24
Vlan Sistemas	192.168.15.0/24
Grupo producción	
Vlan producción	192.168.16.0/24
wifi_produccion	192.168.20.0/24
Vlan Laboratorio	192.168.17.0/24
Vlan Gerencia	192.168.18.0/24

Vlan Cámaras	192.168.21.0/24
Sucursales_Remotas	
Sucursal_Pedernales	192.168.3.0/24
Sucursal_Hualtaco	192.168.2.0/24
Sucursal_SanVicente	192.168.4.0/24
Sucursal_machala	192.168.1.0/24

Tabla 2.3.4.- Segmentación de la Red

2.3.5.- Configuración de Políticas de seguridad en el firewall

En el proceso de configuración de políticas de seguridad en el firewall se tomará en cuenta el siguiente procedimiento:

- Creación de Objetos
- Definición de Políticas de Acceso Wan
- Definición de Políticas de Acceso Lan
- Definición de Políticas de Filtrado
- Configuración de Módulo IPS

2.3.5.1 Creación de Objetos

Para obtener el mayor rendimiento en la aplicación de políticas se establecen los siguientes objetos basados en Dispositivos y Servicios dentro de la red.

2.3.5.1.1 Servidores

IP SERVIDORES	SERVICIO	TIPO	DESCRIPCIÒN
192.168.10.68	Active Directory	Virtual	SRV_directorio_activo
192.168.10.66	Base de Datos , SASF, Web Service	Físico	SRV_Base_datos
192.168.10.58	Correo Electrónico	Virtual	SRV_correo

192.168.10.67	File server	Físico	SRV_file_server
192.168.10.59	App Impuestos	Virtual	SRV_app
192.168.10.16	Antivirus	Virtual	SRV_Antivirus
192.168.10.101	Termometría	Físico	SRV_Termometria
192.168.10.104	Balanza de Pesaje	Físico	SRV_Balanza
192.168.10.106	Cuarto control	Físico	SRV_WINCC_2
192.168.10.108	Producción	Físico	SRV_PLC_1
192.168.10.111	Laboratorio	Físico	SRV_NIR
192.168.10.199	Cuarto control	Físico	SRV_WINCC_1
192.168.10.200	Producción	Físico	SRV_PLC_2
192.168.10.201	Cuarto control	Físico	SRV_WINCC_3
192.168.10.202	Cuarto control	Físico	SRV_siemens
192.168.10.6	Central Telefónica GYE	Físico	SRV_CentralIP

Figura 2.3.5.1.1.-Servidores

2.3.5.1.2 Dispositivos inalámbricos

IP DISPOSITIVOS INALAMBRICOS	DESCRIPCION	PROPAGA
192.168.11.8	Access Point Administrativo	TODAS LAS VLANS
192.168.11.9	Router administrativo	VLAN ADMINISTRACION
192.168.16.8	Access Point producción	TODAS LAS VLANS
192.168.16.9	Router Comedor	VLAN PRODUCCION
192.168.16.10	Router Pesaje	VLAN PRODUCCION

Tabla 2.3.5.1.2.- Dispositivos inalámbricos

2.3.5.1.3 Impresoras

IP IMPRESORAS	AREA	DESCRIPCION
192.168.14.10	Contabilidad	Impresora_contabilidad
192.168.14.11	Administración	Impresora_administracion
192.168.14.12	Producción	impresora_produccion

192.168.14.13	Pesaje	impresora_servicliente

Tabla 2.3.5.1.3.- Impresoras

2.3.5.1.4 Biométricos

IP BIOMÉTRICOS	DESCRIPCIÓN
192.168.11.6	reloj_administrativo
192.168.11.7	reloj_produccion
192.168.11.8	reloj_comedor
192.168.11.9	reloj_garita
192.168.10.17	reloj_sistemas

Tabla 2.3.5.1.4.-Biométricos

2.3.5.1.5 Cámaras

IP CÁMARAS	DESCRIPCIÓN
192.168.21.8	DVR_planta

192.168.21.9	DVR_administrativo
192.168.21.10	DVR_perimetral

Tabla 2.3.5.1.5.-Cámaras

2.3.5.2 Definición de políticas de Acceso

En base a los objetos creados se establecen políticas restrictivas en base a los servicios necesarios de cada subred previamente configurada tal y como se muestra en la tabla a continuación:

DESDE	HASTA	USUARIO	FUENTE	DESTINO	SERVICIO	ACCESO
Grupo administración	Vlan Servidores	any	any	SRV_directorio_activo	any	allow
				SRV_Base_datos	any	allow
				SRV_correo	any	allow
				SRV_file_server	any	allow
				SRV_Antivirus	any	allow
				SRV_CentralIP	any	allow

				AP_Administrativo	any	allow
				Router_administrativo	any	allow
	Vlan Impresoras	any	usr_contabilidad	Impresora_contabilidad	any	allow
	Vlan Impresoras	any	usr_administracion	Impresora_administracion	any	allow
	Vlan VoIP	any	any	any	any	allow
Vlan Gerencia	Vlan servidores	any	any	SRV_directorio_activo	any	allow
				SRV_Base_datos	any	allow
				SRV_correo	any	allow
				SRV_file_server	any	allow
				SRV_Antivirus	any	allow
				SRV_CentralIP	any	allow
				AP_Administrativo	any	allow
				Router_administrativo	any	allow

	Vlan Impresoras	any	any	Impresora_administracion	any	allow
	Vlan VoIP	any	any	any	any	allow
	Vlan Cámaras	any	any	any	any	allow
Sucursales_Remotas	Vlan Servidores	any	any	SRV_directorio_activo		
				SRV_Base_datos		
				SRV_correo		
				SRV_file_server		
				SRV_Antivirus		
Vlan Sistemas	any	any	any	any	any	allow
Grupo producción	Vlan Servidores	any	any	SRV_directorio_activo	any	allow
				SRV_Base_datos	any	allow
				SRV_correo	any	allow
				SRV_file_server	any	allow

				SRV_Antivirus	any	allow
				SRV_CentralIP	any	allow
				Ap_produccion	any	allow
				Router_Comedor	any	allow
				Router_Pesaje	any	allow
				SRV_Termometria	any	allow
				SRV_Balanza	any	allow
				SRV_WINCC_2	any	allow
				SRV_PLC_1	any	allow
				SRV_pantalla_tactil 1	any	allow
				SRV_pantalla_tactil 2	any	allow
				SRV_pantalla_tactil 3	any	allow
				SRV_WINCC_1	any	allow
				SRV_PLC_2	any	allow
				SRV_WINCC_3	any	allow

				SRV_siemens	any	allow
	Vlan Impresoras	any	any	impresora_produccion	any	allow
	Vlan VoIP	any	any	any	any	allow
Vlan Laboratorio	Vlan Servidores	any	any	SRV_directorio_activo	any	allow
				SRV_Base_datos	any	allow
				SRV_correo	any	allow
				SRV_file_server	any	allow
				SRV_Antivirus	any	allow
				SRV_CentralIP	any	allow
				Ap_produccion	any	allow
				Router_Comedor	any	allow
				Router_Pesaje	any	allow
				SRV_NIR	any	allow
	Vlan VoIP	any	any	any	any	allow
Vlan	vlan	any	seguridad	any	any	allow

Administración	camaras					
Vlan producción	Sucursal_machala	any	usr_**mantenimiento**	any	any	allow
Vlan producción	vlan_camaras	any	usr_produccion	dvr_planta	any	allow
				dvr_perimetral	any	allow
vlan producción	vlan_camaras	any	usr_administrativo	dvr_administrativo	any	allow
Vlan Administración	vlan_servidores	any	usr_rrhh	reloj_administrativo	any	allow
				reloj_produccion	any	allow
				reloj_comedor	any	allow
				reloj_garita	any	allow

Tabla 2.3.5.2.-Definición de políticas de Acceso

2.3.5.3. Definición de políticas de Filtrado

Como parte del proceso de configuración de políticas es necesario establecer filtros de navegación en el módulo Url Filtering para el

servicio de internet de la organización, por cuanto se establecen perfiles de usuario a los cuales vamos a delimitar el acceso dependiendo de su uso:

GRUPO DE USUARIOS	PERFIL	DESCRIPCION
Vip	ACCESO_TOTAL	Acceso total , excepción listas negras y páginas prohibidas
Administrativo	ACCESO_CONTROLADO	Sin Redes Sociales , Sin Multimedia , lista negras y páginas prohibidas
Invitados	ACCESO_RESTRINGIDO	Sin acceso a la red Interna + ACCESO_CONTROLADO

Tabla 2.3.5.3.- Definición de políticas de Filtrado

2.3.6.- Configuración de módulo IPS

El módulo IPS que se encuentra dentro de la red desmilitarizada (DMZ), tiene como propósito crear un control adicional en caso que un hacker logre penetrar en el firewall, ya que en ese momento el IPS emitirá una alerta y va a descartar los paquetes sospechosos. El

servidor IPS se va a configurar para que recolecte información sobre eventos sospechosos y los guarde en una base de datos para realizar los reportes.

2.4.- Esquema de Monitoreo

Es importante diseñar un esquema de monitoreo de la red para tener la certeza de que el esquema de seguridad perimetral está funcionando correctamente y se considera “seguro”, por tanto se ha implementado un servidor con el propósito de monitorear la red de la organización.

2.4.1.- Componentes de monitoreo

El servidor de monitoreo contiene las siguientes herramientas de tipo open source:

- NTOP
- NAGIOS
- NEXPOSE

2.4.1.1.- Ntop

La herramienta NTOP sirve para el monitoreo del tráfico de red, es muy útil cuando se tiene tiempos de respuesta altos en la red y se sospecha que, por ejemplo, una estación de trabajo está consumiendo la mayor parte del ancho de banda y está causando

un cuello de botella en la red. NTOP es fácil de usar y presenta información bastante útil como:

- Sesiones TCP activas: Detalle del origen y destino de transmisión de datos de cada host.
- Matriz de conexión: Detalle de las conexiones de hosts a servidores y la cantidad de tráfico intercambiado.
- Monitoreo de los hosts específicos: Detalle de la cantidad de tráfico intercambiada por un host específico.

  Se propone seguir el siguiente esquema de monitoreo para la herramienta NTOP:

- Monitorear las sesiones TCP activas diariamente en la hora pico del uso de red.
- Monitorear la matriz de conexión cuando se detecte que la red tiene tiempos de respuesta altos.
- Monitorear la matriz de tiempos semanalmente para verificar que el uso de la red sea mínimo fuera del horario laborable.

2.4.1.2.- Nagios

La herramienta NAGIOS sirve para monitorear la disponibilidad de hosts y servicios en una red, incluso se pueden monitorear componentes de red como switches. El uso de la herramienta es

muy sencillo y no requiere mucho tiempo para familiarizarse con ella. El esquema de monitoreo de disponibilidad establecido es el siguiente:

EQUIPO	SERVICIOS	ALARMA
SRV_LOG	HTTP	Servicio no esté subido
	PARTICION USUARIO ROOT	80% lleno
	SSH	Servicio no esté subido
	PROCESOS	Más de 100 Procesos
	USUARIOS CONECTADOS	Más de 20 Usuarios
	PING	No responda
SRV_MONITOREO	HTTP	Servicio no esté subido
	PARTICION USUARIO ROOT	80% lleno
	SSH	Servicio no esté subido
	PROCESOS	Más de 100 Procesos

	USUARIOS CONECTADOS PING	Más de 20 Usuarios No responda
SRV. CORREO	HTTP PROCESOS PING	Servicio no esté subido Más de 100 Procesos No responda
SRV. DOMINIO	HTTP PROCESOS PING	Servicio no esté subido Más de 100 Procesos No responda
SRV_MPLS	HTTP PROCESOS PING	Servicio no esté subido Más de 100 Procesos No responda
SRV_BRILL		

	HTTP PROCESOS PING	Servicio no esté subido Más de 100 Procesos No responda
SWITCH ADMINISTRATIVOS	PING	No responda

Tabla 2.4.1.2. Nagios

2.4.1.3.-Nexpose

Es necesario escanear permanentemente los hosts de toda la red para buscar vulnerabilidades en cada uno de sus componentes, generalmente éstas son causadas por la falta de actualización del sistema operativo de cada equipo, es por esto que se propone el siguiente esquema de monitoreo:

- Escanear mensualmente, fuera de horario laborable, todos los hosts de la red
- Actualizar los sistemas operativos de los hosts con mayor número de vulnerabilidades.

- Actualizar semanalmente los plugins de Nexpose para tenerlos actualizados y poder detectar las vulnerabilidades más recientes.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS.

3.1.- Informes iniciales.

Posterior a la implementación del esquema de seguridad perimetral, ya se cuenta con los primeros resultados exitosos, en donde se puede validar la configuración correcta de políticas de comunicación y acceso tal como lo demuestran las siguientes tablas resumidas en base a informe de archivos logs del firewall.

3.1.1. Informe de Accesos

FECHA	PRIORIDAD	CATEGORIA	MENSAJE	FUENTE	DESTINO	ACCION
30/07/2015 10:56	notice	Firewall	Match default rule, DROP	192.168.11.15:54823	192.168.10.254:161	ACCESS BLOCK
30/07/2015 10:56	notice	Firewall	Match default rule, DROP	192.168.11.15:54823	192.168.10.253:161	ACCESS BLOCK
30/07/2015 10:56	notice	Firewall	Match default rule, DROP	192.168.11.15:54823	192.168.10.252:161	ACCESS BLOCK
30/07/2015 10:56	notice	Forward web sites	comcluster.cxense.com	192.168.11.19:57744	23.92.189.52:80	WEB FORWARD
30/07/2015 10:56	notice	Forward web sites	ae9e880c1ae157ca42a7c14b13ce40c1c.profile.icn51.cloudfront.net	192.168.11.19:57737	54.182.152.45:80	WEB FORWARD
30/07/2015 10:56	notice	Forward web sites	us.img.e-planning.net	192.168.11.19:57739	173.193.144.5:80	WEB FORWARD
30/07/2015 10:56	notice	Forward web sites	webdesignec.com	192.168.11.19:57735	50.63.221.1:80	WEB FORWARD
30/07/2015 10:56	notice	Firewall	Match default rule, DROP	192.168.16.100:59817	192.168.11.252:161	ACCESS BLOCK
30/07/2015 10:56	notice	Forward web sites	ads.us.e-planning.net [count=2]	192.168.11.19:57731	75.126.225.196:80	WEB FORWARD
30/07/2015 10:56	notice	Forward web sites	go.microsoft.com	192.168.18.102:50973	23.72.232.49:80	WEB FORWARD
30/07/2015 10:56	notice	Forward web sites	static.hogarutil.com	192.168.11.42:51919	194.30.59.6:80	WEB FORWARD
30/07/2015 10:56	info	DHCP	Sending ACK to 192.168.18.102			DHCP ACK
30/07/2015 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11.12:65378	192.168.18.100:445	ACCESS BLOCK
30/07/2015 10:56	info	Application Patrol	Service=gnutella Mode=port-less Rule=default Access=drop	192.168.11.174:1901	192.168.10.68:88	ACCESS BLOCK
30/07/2015 10:56	notice	Forward web sites	www.littlebigflat.com	192.168.11.42:51918	206.130.122.103:80	WEB FORWARD
30/07/2015 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11.12:65377	192.168.18.100:445	ACCESS BLOCK
30/07/2015 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11.21:50814	192.168.10.252:9100	ACCESS BLOCK

30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11. 42:51917	192.168.10. 253:9100	ACCESS BLOCK
30/07/20 15 10:56	notice	Forward web sites	www.huntermonitoreo.com	192.168.11. 41:50614	200.25.203. 17:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	gd4.alicdn.com	192.168.11. 42:51915	200.196.22 5.120:80	WEB FORWARD
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP	192.168.16. 101:65345	192.168.10. 251:161	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11. 15:50792	192.168.10. 254:9100	ACCESS BLOCK
30/07/20 15 10:56	alert	Blocked web sites	platform.twitter.com: Social Networking	192.168.11. 21:50811	199.96.57.6 :80	WEB BLOCK:BL UECOAT
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.11. 102:54565	192.168.10. 253:9100	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.11. 29:2762	192.168.10. 254:9100	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=6]	192.168.12. 117:5062	192.168.1.3 :5060	ACCESS BLOCK
30/07/20 15 10:56	alert	Blocked web sites	pagead2.googlesyndication.com: Web Advertisements	192.168.11. 29:2761	173.194.12 1.13:80	WEB BLOCK:BL UECOAT
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.16. 106:3280	192.168.11. 252:9100	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.11. 16:1048	192.168.10. 254:161	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.17. 8:64685	192.168.10. 253:161	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.16. 106:3279	192.168.10. 251:9100	ACCESS BLOCK
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=2]	192.168.11. 12:137	192.168.18. 100:137	ACCESS BLOCK
30/07/20 15 10:56	notice	Forward web sites	cdn.syndication.twitter.com	192.168.11. 19:57718	199.96.57.8 :80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	images.taboola.com [count=4]	192.168.11. 19:57550	23.1.8.31:8 0	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	static.addtoany.com	192.168.11. 19:57707	94.31.29.40 :80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	comcluster.cxense.com	192.168.11. 19:57705	23.92.189.5 2:80	WEB FORWARD

30/07/20 15 10:56	notice	Forward web sites	www.microsoft.com	192.168.18. 102:50972	23.195.90.1 51:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	us.img.e-planning.net	192.168.11. 19:57702	173.193.14 4.5:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	crl.microsoft.com [count=10]	192.168.18. 102:50971	165.254.24 4.170:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	a4ee2989bf7311a0dc451fc2e321336 8e.profile.sfo9.cloudfront.net	192.168.11. 19:57700	54.230.118. 168:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	webdesignec.com	192.168.11. 19:57695	50.63.221.1 :80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	ads.us.e-planning.net [count=2]	192.168.11. 19:57693	75.126.225. 196:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	www.bing.com	192.168.11. 21:50798	204.79.197. 200:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	otf.msn.com	192.168.11. 21:50799	137.116.81. 24:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	otf.msn.com [count=4]	192.168.11. 21:50800	137.116.81. 24:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	api.bing.com	192.168.11. 21:50801	191.234.5.8 0:80	WEB FORWARD
30/07/20 15 10:56	notice	Forward web sites	otf.msn.com	192.168.11. 21:50797	137.116.81. 24:80	WEB FORWARD
30/07/20 15 10:56	alert	Blocked web sites	static.chartbeat.com: Web Advertisements(cache hit)	192.168.11. 21:50794	23.79.205.1 51:80	WEB BLOCK:BL UECOAT
30/07/20 15 10:56	notice	Forward web sites	otf.msn.com [count=2]	192.168.11. 21:50793	137.116.81. 24:80	WEB FORWARD
30/07/20 15 10:56	notice	Firewall	Match default rule, DROP [count=3]	192.168.17. 8:50674	192.168.10. 253:9100	ACCESS BLOCK

Tabla 3.1.1. Informe de Accesos

3.1.2. Informe de Filtro de Contenido

Web Request Statistics

Total Web Pages Inspected:

931488

Blocked:

86526

Warned:

647

Passed:

844315

Category Hit Summary

Security Threat (unsafe):

433

Managed Web Pages:

931055

Block Hit Summary

Web Pages Warned by Category Service:

86526

Web Pages Blocked by Custom Service:

0

Restricted Web Features:

0

Forbidden Web Sites:

0

URL Keywords:

0

3.1.2. Informe de Restricción de patrones

SERVICE	FORWARDED DATA	DROPPED DATA	REJECTED DATA
WhatsApp-M	413900	0	0
WeChat-M	23	0	0
Snapchat-M	0	7233	0
BitTorrent-Series	0	1326	0
Gnutella	0	15812	0
QQDownload	2	0	0
GNUnet	0	26	0
Ares	0	593	0
uTorrent	0	9	0
FTP-Applications	30656	0	0
Web-File-Transfer	7109036	0	0
OneDrive	113	0	0

Docstoc	1	0	0
Scribd	146	0	0
Dropbox	171924	0	0
iCloud	18045	0	0
Windows-Media-Player	122	0	0
RealPlayer	19	0	0
PPTV-PPLive	6738	0	0
iTunes	659998	0	0
Adobe-Flash	17	0	0
Dailymotion	3556	0	0
Ooyala	187	0	0
Photobucket	961	0	0
RTSP	39014168	0	0
MP4	550889	0	0
FLV	2753030	0	0
Web-Streaming	163861	0	0
RTMP	54614	0	0
VLC	1	0	0
Youtube	26027090	1038	0
SWF	3957	0	0
MP3	3	0	0
MOV	1	0	0
Spotify	13899	0	0

LastFM	334	0	0
Netflix	178	0	0
Microsoft-Silverlight	18	0	0
Vimeo	1940	0	0
SMTP	975223	0	0
POP3	64122	0	0
Hotmail	125971	0	0
Gmail	20545	0	0
Skype	78082	0	0
H-323	113	0	0
SIP	4668006	0	0
LINE-M	111	0	0
Viber-M	407	0	0
XBOX	35	0	0
SNMP	28898	0	0
DNS	54880	0	0
DCE-RPC	201789	0	0
SMB	8319731	0	0
ICMP	303824	0	0
TeamViewer	494816	0	0
MS-Remote-Desktop-Protocol-RDP	1892	0	0
Secure-Shell-SSH	19357	0	0
LogMeIn	0	26947	0

HTTP-Proxy-Server	9	0	0
Google-Chrome	749676	0	0
Google-translate	1815	0	0
Mozilla-Firefox	164077	0	0
Apple-Safari	34862	0	0
PayPal-com	127	0	0
Evernote	26	0	0
Google-analytics	3851	0	0
ActiveX	615	0	0
Java-Applet	43	0	0
Microsoft-Live-com	3601	0	0
Windows-Store	15528	0	0
AppStore	3055	0	0
Adobe-com	179879	0	0
HTTP-misc	1062131	0	0
RSS	90	0	0
WeatherBug	1	0	0
Wikipedia	8439	0	0
Amazon	98429	0	0
Yahoo	6770	0	0
Microsoft-Windows-Update	520209	0	0
Yum	47	0	0
Adobe	42	0	0

Kaspersky	946	0	0
NOD32	758	0	0
Avast	5435	0	0
Avira	15	0	0
Duba	731	0	0
Apple	13	0	0
Google-Update	6	0	0
WebSphere	9	0	0
TCP-Port-Service-Multiplexer	0	0	0
Domain-Name-Server	1097	0	0
WWW-HTTP	77506	0	0
Torpark	0	0	0
XFER-Utility	1	0	0
Kerberos	168186	0	0
SU-MIT-Telnet-Gateway	3	0	0
NTP	3656	0	0
NCS-local-location-broker	708	0	0
NetBIOS-Session-Service	15608	0	0
Lightweight-Directory-Access-Protocol	32700	0	0
Workstation-Solutions	4	0	0
HTTP-Protocol-over-TLS-SSL	3504404	0	0
Win2k-plus-Server-Message-Block	3513514	0	0
SMTP-Protocol-over-TLS-SSL-was-	17752	0	0

SSMTP			
Real-Time-Stream-Control-Protocol	36	0	0
IDEAFARM-CHAT	7832	0	0
IMAP4-Protocol-over-TLS-SSL	809	0	0
POP3-Protocol-over-TLS-SSL	372437	0	0
Microsoft-Authentication-via-SSL	38025	0	0
Google-SSL	717130	0	0
Yahoo-Authentication-via-SSL	72830	0	0
SOAP	14	0	0
TFTP	26	0	0
MicrosoftOnline-Authentication-via-SSL	30	0	0
Microsoft-WINS	0	0	0
SSL-TLS	19359398	0	0
Google-APIs-SSL	28851	0	0
Google-App-Engine-SSL	64051	0	0
Google-User-Content-SSL	192169	0	0
Apple-iMessage	7453	0	0
QQ-Private-Protocol	2183	0	0
Thunder-Private-Protocol	0	0	0
Jabber-Private-Protocol	7961	0	0
Facebook	437227	59350	0
Flickr	0	9	0
Linkedin	4445	0	0

Twitter	148552	0	0
Pinterest	1038	0	0
Tumblr	5108	0	0
VKontakte	15	0	0
Instagram	260974	0	0
other	6636724	0	0

CONCLUSIONES.

1. El resultado de los informes del Firewall confirman la ejecución correcta de la configuración de políticas de acceso Wan y Lan aplicadas

2. El resultado de los informes del Firewall confirman la ejecución exitosa de políticas de acceso a la navegación en internet

3. El resultado de los informes del Firewall confirman la ejecución exitosa de políticas de patrones a la navegación en internet

4. La segmentación de la red dio como resultado el acceso a los servicios de red solo a personal autorizado minimizando el riesgo de los activos informáticos.

RECOMENDACIONES

1. Se recomienda realizar monitoreo permanente de los accesos a la red para precautelar el óptimo funcionamiento del firewall.

2. Se recomienda segmentar los servicios de red identificando puertos necesarios para la ejecución de aplicaciones críticas a las cuales los usuarios y proveedores tienen acceso, para incrementar la eficiencia de los accesos y evitar posibles ingresos no deseados a la red de la organización.

3. Se recomienda realizar un hardening de servicios a los servidores de la organización para evitar aperturas de puertos no deseados.

4. Se recomienda documentar e implementar una política de respaldos para salvaguardar la información y la configuración de cada uno de los servicios alojados en los servidores de la organización.

5. Se recomienda complementar el esquema de seguridad perimetral con una adecuada política de contingencia y alta disponibilidad de los activos informáticos.

BIBLIOGRAFÍA

Sedo-Help. (Julio de 2015). Obtenido de https://sedo-es1.custhelp.com/

ServiLinux. (Julio de 2015). Obtenido de http://servilinux.galeon.com/

wikipedia. (Julio de 2015). Obtenido de https://es.wikipedia.org/

IBM. (s.f.). *Configuring the X-Force Virtual Patch.* Recuperado el Abril de 2015, de http://www-01.ibm.com/support/knowledgecenter/SSB2MG_4.6.2/com.ibm.ips.doc/tasks/configuring_xforce_blocking.htm

IBM. (s.f.). *Data loss prevention, important consideration.* Recuperado el Abril de 2015, de http://www-01.ibm.com/support/knowledgecenter/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/content_analyzer_important_considerations.htm

IBM. (s.f.). *IBM X-Force*. Recuperado el Abril de 2015, de IBM Security Network Intrusion Prevention System (IPS) V4.6.1 documentation: http://www-03.ibm.com/security/xforce/

UNIVERSIDAD INTERNACIONAL SEK. (2008). *ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK – ECUADOR.* Quito.

Universidad Técnica del Norte de España. (2013). *SEGURIDAD PERIMETRAL PARA LA RED DE DATOS.*