ANÁLISIS Y DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA REDES DE DATOS MEDIANTE ENFOQUES ISO 27001 Y LA UTILIZACIÓN DE TÉCNICAS DE DEFENSA. CASO DE ESTUDIO: EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN NICOLÁS

GUILLERMO LEÓN GARCÍA SOTO

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PLANETA RICA - CÓRDOBA
2015

ANÁLISIS Y DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA REDES DE DATOS MEDIANTE ENFOQUES ISO 27001 Y LA UTILIZACIÓN DE TÉCNICAS DE DEFENSA. CASO DE ESTUDIO: EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN NICOLÁS

GUILLERMO LEÓN GARCÍA SOTO

TRABAJO PRESENTADO AL DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES, EN CUMPLIMIENTO PARCIAL DE LOS REQUISITOS PARA OBTENER EL GRADO DE INGENIERO DE SISTEMAS

DIRECTOR:
ING. M.SC. JORGE GOMEZ GOMEZ

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PLANETA RICA CÓRDOBA
2015

NOTA ACEPTACION

_____

Director

_____

Jurado

_____

Jurado

DEDICATORIA

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres.

Por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

A mi esposa Mónica Ramos.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por su incondicionalidad, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis familiares.

A mis hijos María Catalina y José Guillermo por su apoyo y comprensión; a mi hermana Catia, a mi tío Oscar, a mi cuñada María José y a todas y cada una de las personas que de alguna u otra manera contribuyeron a que lograra esta meta que me propuse en la vida y que me ha permitido crecer intelectualmente como persona y como ser humano.

Guillermo León García Soto.

AGRADECIMIENTOS

A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi tutor ING. M.SC. Jorge Gomez Gomez, quien siempre estuvo dispuesto a colaborarme y a compartir sus conocimientos.

A Marino Moreno Rhenals, quien con su conocimiento me guio y apoyo en este proyecto.

A la Universidad de Córdoba, facultad de ingeniería de sistemas y telecomunicaciones porque con ella mi sueño es una realidad, especialmente a nuestro Decano Ing. Daniel Sala por su actitud de escucha y comprensión cuando lo necesitamos.

Un especial agradecimiento a todo el personal de la E.S.E Hospital San Nicolás donde realicé mi trabajo por todo el apoyo que me brindaron, especialmente Luis Alfredo Callejas Callejas, Over Fernádes Barreto y al Doctor Rafael Pedro Marques gerente de la E.S.E. Mil gracias.

A todas las personas que de alguna u otra forma contribuyeron con migo, reciban este trabajo como suyo y sépanse acreedores de mi especial agradecimiento: Dios los bendiga.

¡Gracias a ustedes!

Guillermo León García Soto.

TABLA DE CONTENIDO

1. RESUMEN....14
2. INTRODUCCION....15
3. OBJETIVOS....17
3.1. General....17
3.2. Específicos....17
4. CAPÍTULO 0. FUNDAMENTOS TEÓRICOS SOBRE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).....18
4.1. Antecedentes históricos....18
4.2. Antecedentes Investigativos....29
4.2.1. Contexto Internacional....29
4.2.2. Contexto Nacional....31
4.2.3. Contexto Local....33
4.3. Sistema Gestión de Seguridad de la información (SGSI)....33
4.3.1. Consideraciones Generales....34
4.3.2. Ciclo de vida de la seguridad....37
4.3.3. Marco Legal....42
4.4. Políticas de Seguridad de la Información....43
4.5. Norma ISO 27000....45
4.6. Firewall....46
4.7. Sistema de Detección de Intrusos IDS....47
4.8. Sistema de Prevención de Intrusos IPS....49
4.9. Proxy....50
5. CAPITULO I. ANALISIS DEL RIESGO EXISTENTE EN LA RED DE DATOS DE LA E.S.E. HOSPITAL SAN NICOLÁS.....52

5.1. Inventario de Activos 52
5.2. Esquema de la red de datos del Hospital San Nicolás de Planeta Rica. 56
5.3. Análisis de Riesgo 56
5.3.1. Análisis de la situación 56
5.3.2. Risk-Defense 57
5.3.3. Madurez de la seguridad 58
5.3.4. Tarjeta de puntuación 59
5.3.5. Iniciativas de seguridad 60
5.3.6. Evaluación detallada 60
5.3.7. Análisis de la evaluación 62
5.3.8. Aplicaciones 74
5.3.9. Operaciones 80
5.3.10. Personal 87
5.3.11. Lista de acciones recomendadas 91
5.3.12. Apéndices 93
5.3.13. Interpretación de gráficos 99
5. CAPITULO II. DISEÑO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICADA A E.S.E. HOSPITAL SAN NICOLÁS. 100
5.3. Generalidades 100
5.4. Alcance de Las Políticas 101
5.5. Objetivo de las Políticas 101
5.6. Análisis de las razones que impiden la aplicación de las Políticas de seguridad informática. 102
5.7. Responsabilidades 103
5.8. Definición de Políticas de Seguridad Informática 103
5.9. Disposiciones Generales 103

5.9.2. Comité 104
5.9.3. Administración de informática 104
5.9.4. Lineamientos para la adquisición de bienes informáticos 105
5.9.5. Precio. 106
5.9.6. Calidad 106
5.9.7. Experiencia 106
5.9.8. Desarrollo Tecnológico 106
5.9.9. Estándares 106
5.9.10. Capacidades 106
5.9.11. Instalaciones de los equipos de cómputo 110
5.9.12. Lineamientos en Informática: Información 110
5.9.13. Funcionamiento de los equipos de cómputo 112
5.9.14. Plan de contingencias informáticas 113
5.9.15. Estrategias informáticas 114
5.9.16. Acceso Físico 114
5.9.17. Identificadores de usuario y contraseñas 114
5.9.18. Responsabilidades Personales 115
5.9.19. Salida de Información 117
5.9.20. Uso apropiado de los recursos 118
5.9.21. Queda Prohibido 118
5.9.22. Software 119
5.9.23. Recursos de red 119
5.9.24. Conectividad a internet 120
5.9.25. Actualizaciones de la política de seguridad 121
5.9.26. Disposiciones Transitorias 121

5.9.27. Beneficios de implantar políticas de seguridad informática 122

6. CAPITULO III. IMPLEMENTACIÓN EN SERVIDORES VIRTUALES DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA GESTIÓN Y ADMINISTRACIÓN DE LA RED DE DATOS DE E.S.E. HOSPITAL SAN NICOLÁS. 122

6.1. Nuevo escenario de la red de datos del Hospital San Nicolás de planeta Rica. 123

6.2. Manual de Instalación y configuración de Endian Firewall UTM..... 124

6.2.1 Configuración firewall Endian 137

6.2.2 Configuración Proxy Web Endian 151

7. CONCLUSIONES 170

8. BIBLIOGRAFIA.....172

INDICE DE ILUSTRACIONES

Ilustración 1. Área de Protección 36
Ilustración 2. Ciclo de Vida de la Seguridad 37
Ilustración 3. Firewall 47
Ilustración 4. Red de datos Hospital San Nicolás de Planeta rica 56
Ilustración 5. Risk-Defense 57
Ilustración 6. Nuevo escenario de la red del Hospital San Nicolás de Planeta Rica123
Ilustración 7. Selección del idioma 124
Ilustración 8. Mensaje de bienvenida Endian 124
Ilustración 9. Formateo del disco 125
Ilustración 10. Activar servicios de consola 125
Ilustración 11.Progreso de instalacion endian 126
Ilustración 12. Instalando paquetes.....126
Ilustración 13. Configuración IP 126
Ilustración 14. Reinicio del sistema 127
Ilustración 15. Inicio Endian 127
Ilustración 16. Verificación de IP 128
Ilustración 17. Bienvenida de Endian 128
Ilustración 18. Selección de idioma de configuración Endian 129
Ilustración 19. Licencia de uso Endian 129
Ilustración 20. Restablecer configuración Endian.....130
Ilustración 21. Configuración de contraseñas Endian.....130
Ilustración 22. Tipo de conexión de la interfaz 131
Ilustración 23. Tarjetas de red.....131
Ilustración 24. Interfaz de red 1.....132
Ilustración 25. Interfaz de red 2.....132
Ilustración 26. Configuración de interfaz de red 133
Ilustración 27. Configuración IP y DNS 133
Ilustración 28.Configuración de administrador 134
Ilustración 29. Guardar las configuraciones 134

Ilustración 30. Reinicio del sistema 135
Ilustración 31. Login endian 135
Ilustración 32. Consola de administración de Endian 136
Ilustración 33. Verificación de funcionamiento de Endian 136
Ilustración 34. Opción cortafuegos 137
Ilustración 35. Pestaña NAT fuente 138
Ilustración 36. Tipo redIP 138
Ilustración 37.Añadir regla NAT LAN-Internet 139
Ilustración 38. Crear regla NAT LAN-Internet 139
Ilustración 39. Aplicar regla NAT LAN-Internet 140
Ilustración 40. Añadir regla NAT DMZ-Internet 140
Ilustración 41. Aplicar regla NAT DMZ-Internet 141
Ilustración 42. Origen Tipo Roja 141
Ilustración 43. Destino Zona Verde 142
Ilustración 44. Política acción denegar 142
Ilustración 45. Aplicar regla denegar roja-verde 143
Ilustración 46. Crear nueva regla port forwarding / destination nat 143
Ilustración 47. Seleccionar enlace activo principal 144
Ilustración 48. Seleccionar servicio FTP 144
Ilustración 49. Digitación de IP de servidor 145
Ilustración 50. Crear y aplicar regla 145
Ilustración 51. Crear regla acceso internet - DMZ puerto 80 146
Ilustración 52. Crear y aplicar regla 146
Ilustración 53. Opción tráfico entre zonas 147
Ilustración 54. Añadir nueva regla de cortafuegos inter-zonas 147
Ilustración 55. Seleccionar origen y destino zona / interfaz 148
Ilustración 56. Seleccionar origen naranja y destino verde 148
Ilustración 57. Seleccionar la acción denegar 149
Ilustración 58. Crear y aplicar 149
Ilustración 59. Política de ruteo Internet - Server http 150
Ilustración 60. Opción proxy Endian 151

Ilustración 61. Habilitar proxy HTTP....152
Ilustración 62. Configuraciones de proxy....152
Ilustración 63. Puertos permitidos y puertos ssl....153
Ilustración 64. Configuración del registro....153
Ilustración 65. Proxy transparente Bypass....154
Ilustración 66. Administración cache....154
Ilustración 67. Proxy upstream....155
Ilustración 68. Guardar configuración proxy....155
Ilustración 69. Aplicar configuración proxy....156
Ilustración 70. Pestaña autenticación....156
Ilustración 71. Añadir usuario NCSA....157
Ilustración 72. Datos usuario NCSA....157
Ilustración 73. Guardar usuario NCSA....157
Ilustración 74. Aplicar usuario NCSA....157
Ilustración 75. Pestaña autenticación - administrar grupos....158
Ilustración 76. Añadir grupo NCSA....158
Ilustración 77. Datos grupo NCSA....158
Ilustración 78. Guardar datos grupo NCSA....159
Ilustración 79. Aplicar datos grupo NCSA....159
Ilustración 80. Pestaña contenfilter....159
Ilustración 81. Contenfilter crear perfil....160
Ilustración 82. Nombre del perfil....160
Ilustración 83. Filtrado de contenido Alto....161
Ilustración 84. Denegar contenido pornográfico y juegos....161
Ilustración 85. Listas negras denegar contenido pornográfico, juegos, etc....162
Ilustración 86. Listas negras y listas blancas....162
Ilustración 87. Crear perfil listas negras y listas blancas....163
Ilustración 88. Mensaje de creación de perfil....163
Ilustración 89. Aplicar creación de perfil....164
Ilustración 90. Pestaña política de acceso....164
Ilustración 91. Datos política de acceso....164

Ilustración 92. Selección de filtrobajo 165
Ilustración 93. Guardar política del proxy 165
Ilustración 94. Aplicar política del proxy 166
Ilustración 95. Configuración navegador web mozilla.....166
Ilustración 96. Opciones avanzadas - pestaña red.....167
Ilustración 97. Configuración de conexión.....167
Ilustración 98. Autenticación navegador.....168
Ilustración 99. Denegación youtube 168
Ilustración 100. Denegación facebook 169

INDICE DE TABLAS

Tabla 2. Inventario General de Activos 52
Tabla 3. Inventario detallado de Activos..... 55
Tabla 4. Áreas de Análisis MSAT..... 57
Tabla 5. Madurez de la seguridad..... 58
Tabla 6.Tarjeta de Puntuación 60
Tabla 7. Iniciativas de Seguridad 60
Tabla 8. Áreas de análisis..... 62
Tabla 9. Infraestructura..... 67
Tabla 10. Autenticación 71
Tabla 11. Gestión y Control 74
Tabla 12. Implementación y Uso..... 76
Tabla 13. Diseño de Aplicaciones..... 79
Tabla 14. Almacenamiento y comunicaciones de datos..... 80
Tabla 15. Entorno 81
Tabla 16. Directiva de Seguridad..... 83
Tabla 17. Gestión de actualizaciones y revisiones..... 85
Tabla 18. Copias de seguridad y recuperación 87
Tabla 19. Requisitos y evaluaciones..... 88
Tabla 20. Directiva y procedimientos 90
Tabla 21. Formación y conocimiento 91
Tabla 22. Lista de acciones recomendadas 92
Tabla 23. Preguntas y Respuestas 98
Tabla 24. Glosario..... 99

1. RESUMEN

Hoy día, el desarrollo de las tecnologías de la información y comunicaciones ha impactado en las empresas de los diferentes sectores económicos, convirtiendo la información en uno de los activos más importantes de las empresas, las cuales han optado por implementar plataformas tecnológicas en sus sistemas de negocio, preocupando así a los administradores el salvaguardar y proteger los datos teniendo presente los conceptos de confidencialidad, disponibilidad e integridad, pilares de la seguridad informática, para así generar confianza en los clientes y garantizar la seguridad en la continuidad del negocio.

Es por esto que el hospital San Nicolás ubicado en Planeta Rica – Córdoba, está en proceso de transformación continuo debido a la diversidad de cada una de las dependencias que tienen lugar en el óptimo funcionamiento de esta institución. El hospital cuenta con un Sistema de Información que necesita de niveles de seguridad óptimos para cumplir con todos los parámetros administrativos y la confidencialidad de los datos de los usuarios y entidades del sistema.

Por los motivos mencionados anteriormente es absolutamente imperativo que toda la información de desarrollos, operaciones y mejoramiento continuo que se almacena y procesa en el Sistema de Información esté debidamente asegurada, mediante técnicas que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la misma. En este orden de ideas la solución más acorde para suplir esta necesidad es realizar un análisis profundo de la red de esta dependencia y posteriormente diseñar un modelo de seguridad de la información basado en técnicas de defensa en profundidad.

La siguiente investigación se estructuró en cuatro (4) capítulos, a saber:

La introducción, la cual describe el problema, la pregunta de investigación, la justificación, la metodología y los objetivos.

Capítulo 0. Marco Teórico. En el cual se detalló toda la teoría sobre la que se sustenta esta investigación, con una presentación de los estudios anteriores (antecedentes y estado del arte en el ámbito internacional y nacional) sobre la materia.

Capitulo I. Recolección de datos y análisis de riesgo acerca de la infraestructura informática y de la red de datos que existe actualmente en E.S.E. Hospital San Nicolás.

Capitulo II. Diseño de una guía de políticas de seguridad informática aplicada a E.S.E. Hospital San Nicolás.

Capitulo III. Diseño de un sistema de gestión de seguridad de la información (SGSI) para la protección y control de la red de datos de la E.S.E. Hospital San Nicolás.

2. INTRODUCCION

La Empresa Social del Estado Hospital San Nicolás del Municipio de Planeta Rica (Córdoba), la cual se encuentra ubicada dentro de la Zona Urbana del mismo, está en proceso de transformación continua debido a la diversidad de cada una de las dependencias que tienen lugar en el óptimo funcionamiento de esta institución.

Dentro del marco de las actividades realizadas por la E.S.E. Hospital San Nicolás del municipio de Planeta Rica, se encuentra el consabido Sistema de Información que necesita de niveles de seguridad óptimos para cumplir con todos los parámetros administrativos y la confidencialidad de los datos de los usuarios y entidades del sistema.

Por los motivos mencionados anteriormente es necesario que toda la información de desarrollo, operaciones y mejoramiento continuo que se almacena y procesa en el Sistema de Información esté debidamente asegurada, mediante técnicas que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la misma. En este orden de ideas la solución más acorde para suplir esta necesidad es realizar un análisis

profundo de la red de esta dependencia y posteriormente diseñar un modelo de seguridad de la información basado en técnicas de defensa en profundidad.

Mediante el desarrollo de este modelo, la información que se procesa, almacena y circula dentro de la red de datos de la E.S.E. Hospital San Nicolás podrá adquirir un nivel de seguridad bastante alto y teniendo en cuenta que toda esta información es altamente clasificada, será una solución óptima para mantenerla confidencial, integra y disponible.

Con la implementación de modelo de seguridad basado en el estándar de la ISO 27001 y en técnicas de defensas se pretende que la Empresa Social del Estado Hospital San Nicolás pueda garantizar en un alto grado, la confidencialidad, integridad y disponibilidad de la información que es almacenada y circula constantemente por su red y la cual tiene un alto grado de confidencialidad dada la naturaleza de su contenido.

La implementación del modelo de seguridad es necesario debido a la naturaleza de la información que circula por la red de la Empresa Social del Estado Hospital San Nicolás, pero más importante aún porque la red de datos se encuentra totalmente vulnerable desde el punto de vista de la red LAN, pero también desde Internet.

Por otra parte es necesario optimizar la arquitectura de la red que se tiene actualmente ya que hoy en día no se cuenta con una red segmentada en cuanto a direccionamiento y servicios que pueda satisfacer los requisitos más básicos de una red de datos que soporte el tipo de información que esta debe soportar.

La Empresa Social del Estado Hospital San Nicolás es una empresa del sector de la salud a nivel Municipal en Planeta Rica Córdoba, por su carácter hospitalario maneja información de carácter clasificada y de suma importancia para el desarrollo de sus actividades. Concretamente el problema radica en que no existe una arquitectura de red que ofrezca un mínimo de seguridad para salvaguardar la información que es almacenada y circula por la E.S.E. Hospital San Nicolás.

Teniendo en cuenta que un modelo de seguridad básico tiene como premisa fundamental velar por la confidencialidad, integridad y disponibilidad de la información, es necesario implementar la arquitectura de seguridad propuesto en la E.S.E. Hospital San Nicolás ya que con la red que se tiene actualmente no se asegura ninguna de las características mencionadas ni tampoco se asegura un funcionamiento óptimo de la red actual.

3. OBJETIVOS

3.1. General

Diseñar un modelo de seguridad de la información basado en técnicas de defensa, para el sistema de información del E.S.E. Hospital San Nicolás del Municipio de Planeta Rica.

3.2. Específicos

- Analizar el riesgo existente en la red de datos de la E.S.E. Hospital San Nicolás.
- Diseñar una guía de políticas de seguridad informática aplicada a la E.S.E. Hospital San Nicolás.
- Implementar en servidores virtuales políticas de seguridad informática para la gestión y administración de la red de datos de la E.S.E. Hospital San Nicolás.

4. CAPÍTULO 0. FUNDAMENTOS TEÓRICOS SOBRE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

4.1. Antecedentes históricos

Según Unam (2013) “el surgimiento de la raza humana en el planeta, la información ha estado presente bajo diversas formas y técnicas. El hombre buscaba la manera de representar sus hábitos y costumbres en diversos medios para que pudieran ser utilizados por él y por otras personas”.

La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban en lugares de difícil acceso y sólo las personas autorizadas accedían a ella.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, e incluso en muchos casos, llegando a tener un valor superior. Por ello la seguridad informática es muy importante ya que afecta directamente a gobiernos, institutos, empresas e individuos.

Es importante conocer el surgimiento de la historia de la tecnología, para entender la situación a la que nos enfrentamos hoy en día, por lo que resulta interesante conocer cuántas cosas tuvieron que suceder para llegar hasta lo que hoy tenemos, quiénes fueron las personas que idearon e inventaron los diversos desarrollos tecnológicos e incluso determinar hacia dónde se dirige la tecnología y por supuesto hacia dónde va la seguridad informática.

Para ello, fue indispensable optimizar los recursos tecnológicos con los que se contaba en determinada época de tal manera que se mantuviera un buen sistema de seguridad de la información.

Cabe destacar que este desarrollo tecnológico de la información ha tenido consecuencias debido a que existen personas que buscan la manera de violar la integridad, confidencialidad y disponibilidad de la información que viaja a través de los equipos de comunicación con el fin de realizar acciones indebidas y obtener beneficios personales.

Todos estos acontecimientos que se fueron desarrollando se muestran de manera cronológica. Resulta interesante analizar cómo es que, a través de los años, se han ido logrando varios avances tecnológicos en los diversos países competitivos como Estados Unidos y Japón, cuyo objetivo principal es y seguirá siendo, mantener seguros los sistemas en donde se almacena la información, teniendo una comunicación confiable y segura entre ellos.

En el año 550 aC, primer sistema de correo.

Ciro el Grande, rey de Persia, diseña el primer sistema para transmitir información por postas. Setecientos años después, los chinos también tendrán el suyo a lo grande: 50 mil caballos, 1400 bueyes, 6700 mulas, 400 carros, 6mil botes, 200 perros y 1150 ovejas.

1605. Bacon crea el Alfabeto binario. Bacon describe un modo de representar las letras del alfabeto en secuencias de cifras binarias, sucesiones de ceros y unos, fácilmente codificables y decodificables.

1614. Napier inventa los logaritmos. Descubre este concepto matemático que resultará crucial para la programación de computadoras.

1623. Las Primeras Calculadoras. Wilhelm Schickard construye la primera calculadora mecánica con poleas y engranajes de reloj. El filósofo y matemático Blaise Pascal presenta la Pascalina en 1642.

1726. Llega la primera computadora. Charles Babbage diseña un “motor analítico”, una computadora programable para todo tipo de propósitos. Debido a su funcionamiento a vapor y al hecho de que todas las piezas son fabricadas a mano, el proyecto fracasa. La idea sigue.

1860. Hola, Teléfono. Antonio Meucci es el primer inventor del aparato de comunicación de voz a distancia que patenta el escocés Alexander Graham Bell en abril de 1875.

1946. Primera computadora electrónica. John Presper Eckert y John William Mauchly construyen la ENIAC (Electronic Numerical Integrator And Computer) en la Universidad de Pensilvania. Su propósito: calcular la trayectoria de proyectiles para el laboratorio de balística del ejército. Es totalmente digital. Pesa 27 toneladas, ocupa una superficie de 167m2 y opera con 17,468 válvulas electrónicas.

1950. Computadoras conectándose con otras Computadoras. El proyecto se denomina RAND (Research And Development) y se desarrolla para facilitar el intercambio entre investigadores en inteligencia artificial.

1958. Nace ARPA (Advanced Research Project Agency) El abuelo de Internet. Con el objetivo de impulsar la investigación y el desarrollo tecnológico con fines estratégicos y militares, EE.UU. establece la ARPA, en cuyo seno nace ARPANET, más tarde Internet.

1961. Los paquetes de información inician su viaje. Varios investigadores desarrollan paralelamente la idea de que la información viaje en paquetes. Es decir, conjuntos limitados de datos unidos a la información necesaria para controlarlos. En este desarrollo se destacan dos personajes clave: Vinton Cerf y Robert Kahn.

1969. Atando nodos. En 1969 se creó la primer red de computadoras entre cuatro centros de investigación que conforman históricamente los primero cuatro hosts de Internet que fueron SRI (Stanford Research Institute), UCLA (University of California in los Angeles), UCSB (University of California in Santa Barbara) y la Universidad de Utah. A esta red se le denominó Arpanet (red (net) de arpa).

1970. Alguien escribe una palabra nueva: Internet. Vinton Cerf es considerado la primera persona que acuña el término Internet.

1971. El correo electrónico abre sus puertas. Ray Tomilinson, de la empresa contratada BBN, idea un programa de correo electrónico para enviar mensajes a través de la red.

1972.

- ¿El Primer Virus? De repente, en las pantallas de todas las IBM 360 empieza a aparecer un mensaje: “”I’m a creeper… catch me if you can” (Soy una enredadera. ¡atrápame si puedes!). Robert Thomas Morris es considerado el autor de este mítico virus que da lugar lógicamente, al primer programa antivirus. ¿Cómo se llamará?, algo muy lógico: “Reaper”, es decir, segadora.
- Llega la arroba. Al perfeccionar su programa de correo electrónico, Ray Tomlinson rescata el antiguo símbolo @ para separar el nombre del destinatario del lugar donde se encuentra.

1973. La conexión cruza el océano NORSAR (NOR-wegian Seismic AR-ray), una agencia gubernamental noruega de detección sísmica, fue la primera institución europea que se conectó a la red de ARPANET. Poco después, lo hizo también el University College de Londres.

1975.

- Primer Troyano. John Walker descubre la forma de distribuir un juego en su UNIVAC 1108 e inadvertidamente da origen al primer troyano de la historia llamado “Animal/Pervade”. Animal ya que consistía en que el software debía adivinar el nombre de un animal en base a preguntas realizadas al usuario. Pervade era la rutina capaz de actualizar las copias de Animal en los directorios de los usuarios, cada vez que el mismo era ejecutado.
- Bill Gates funda Microsoft. Microsoft se dedica a desarrollar, fabricar y producir software y equipos electrónicos. A mediados de los 80 domina el mercado de los ordenadores personales con su sistema operativo MS-DOS. En el 2007 registra 80,000 empleados en más de 100 países, así como beneficios anuales superiores a los 50,000 millones de dólares.

1976. Crece una Manzana. Steve Jobs, de 21 años y Steve Wozniak, de 25, diseñan una computadora más pequeña, más barata y más fácil de utilizar que las ya

existentes. Inspirado en el huerto de Oregón donde había trabajado con algunos amigos, Jobs la bautiza con el nombre de “Apple Computer”.

1977. Primera demostración del protocolo TCP/IP. El transmisión Control Protocol / Internet Protocol, abreviado TCP/IP, se caracteriza por un excelente funcionamiento. Es el único conjunto de reglas para el envío de datos que años más tarde aprobó ARPANET.

1978. Y mañana será Spam. Trescientos noventa y tres empleados de ARPANET reciben inesperadamente un correo de la compañía de ordenadores DEC invitándolos al lanzamiento de un nuevo producto. Se trata del primer antecedente del más tarde denominado spam.

1979. Nace Usenet. Tom truscott y Jim Ellis, estudiantes de la Universidad de Duke, crean Usenet. Palabra formada con las primeras letras de Ussers Network; es decir, red de usuarios. Permite enviar y recibir mensajes (denominados artículos) a distintos grupos de noticias, aportando y discutiendo sobre temas determinados.

1982.

- Comienza la invasión de ratones. El primer Mouse de uso doméstico es presentado por Mouse Systemas. Sirve par a la PC de IBM. Su invención original corresponde a Douglas Engelbart y data de 1967,
- Llega Minitel. Este servicio de videotexto mediante redes de teléfono es lanzado en Francia por PPt. Es considerado el servicio online más exitoso hasta el arribo de la World Wide Web.

1983.

- ARPANET se Desmilitariza. En 1983 la parte civil se separó de la parte militar de la Arpanet y nace lo que hoy se le conoce como Internet. Hasta ese entonces ya eran más de 500 nodos conectados a la red. En la época de los años ochenta empieza el crecimiento explosivo de las computadoras personales, esto permitió que muchas compañías se unieran a Internet por primera vez. De esta forma Internet empezó a penetrar en el entorno corporativo apoyando la comunicación en las empresas con sus clientes y proveedores.
- Los virus se hacen Públicos. Keneth Thompson, el creador de UNIX, demuestra públicamente cómo desarrollar un virus informático. Algo similar realiza un año

después el Dr. Fred Cohen en un discurso de agradecimiento con motivo de un homenaje.

- TCP/IP protocolo único. - Seis años después de la primera demostración, los protocolos TCP/IP son los únicos aprobados por ARPANET. Internet pasa a ser "una serie de redes conectadas entre sí, especialmente las que utilizan el protocolo TCP/IP".

1985. La primera PC multimedia. Aunque nace para compartir y suceder a la consola de juegos Atari, la Amiga 1000, creada por Commodore, se convierte en la primera computadora personal "PC" multimedia de gran éxito comercial.

1988. ¡Todos a Chatear! Jarkko Oikarinen desarrolla el "IRC" (Internet Realy Chat), un programa que permite charlar "en vivo en Internet".

1989. Arpanet le da el paso al Internet comercial.

- Tim Berners-Lee, investigador del CERN (Organización Europea para la Investigación Nuclear) en Suiza, estaba desarrollando un sistema de hipertexto, que permitía "navegar" entre documentos por medio de hiperligas de texto e imágenes, con sólo el click de un ratón.
- Un par de años después aparece el primer navegador gráfico (browser) comercial de Internet, el mosaic. Desarrollado por Marc Andreesen y un grupo de estudiantes programadores en la NCSA (National Center for Supercomputing Applications) localizado en la Universidad de Illinois en Urbana Champaign. Internet abrió sus puertas a actividades de tipo comercial y esto ocasionó que nuevos países tuvieran conexión a Internet.

1990. El primer buscador. Buscar y encontrar algo en Internet ya es un problema. La universidad de McGill ofrece el buscador Archie. Al año siguiente llega Wais y Gopher. (Los tres sistemas son anteriores a la www).

1991.

- El texto se vuelve Hipertexto. Tim Berners-Lee mejora la implementación del hipertexto liberándolo al uso público. Mediante el hipertexto el usuario puede saltar de un texto a otro relacionado. La forma más habitual de hipertexto en documentos es la de hipervínculos o referencias cruzadas automáticas que van a otros

documentos. El hipertexto no está limitado a datos textuales, también puede asociar dibujos, sonidos o videos.

- Internet se presenta en sociedad. Vinton Cerf, también conocido como el padre de Internet, crea la Internet Society (ISOC) de la que será presidente entre 1992 y 1995. ISOC es una asociación no gubernamental sin fines de lucro, dedicada exclusivamente al desarrollo mundial de Internet.
- Llega Linux. Cuando el finlandés Linus Torvalds era estudiante de ingeniería de la Universidad de Helsinki crea el nuevo sistema operativo libre.

1993.

- Comienza el Control. La distribución de las direcciones y la administración de las bases de datos constituyen una dificultad creciente. Para administrar la tarea, se crea la InterNIC (Internet Network Information Center).
- Mosaic, primer gran navegador gráfico. Desplazando al Gopher, basado en textos, Mosaic consigue alcanzar gran popularidad: la www se convierte en el acceso preferido a Internet.

1994.

- Ahora se llama Autopista. En una conferencia celebrada en la Universidad de los Ángeles, Al Gore acuña la expresión “autopista de la información” para referirse a lo que las computadoras harán en el futuro. Sin embargo se queda corto.
- Primer spam. La firma de abogados Canter and Siegel aprovecha Usenet para publicar un aviso de sus servicios legales. Inicia así el spam o correo basura: mensajes no solicitados, habitualmente publicitarios, enviados masivamente. Como su mismo nombre indica, resultan muy molestos para el consumidor.
- Primer buscador basado en textos. WebCrawler es creado para rastrear textos y no sólo títulos de páginas web. Con un mecanismo muy similar, otro buscador denominado Lycos se convierte en el primero en obtener éxito comercial.

1995.

- Incrementa el número de países con conexión. El número de países con conexión tuvo un incremento considerable, de 121 a 165 países.

- Netscape, primer Navegador comercial. La compañía Netscape Communications, creado por Marc Andreessen, uno de los creadores de Mosaic, lanza el navegador Netscape.
- Yahoo! Dos estudiantes de ingeniería de la Universidad de Stanford, Jerry Yang y David Filo, dedican muchas horas a la creación de listas de sus sitios preferidos. Los dividen en categorías, subcategorías. Casi sin querer, idean el buscador más exitoso de los primeros tiempos de Internet: Yahoo ("Yet Another Hierarchical Officious Oracle"). Aunque sus autores suelen ofrecer una explicación más sencilla, Yahoo se traduce familiarmente como "tonto" o "torpe".
- Amazon vende su primer libro. La librería virtual Amazon, creada por Jeff Bezos, vende su primer libro. En tan sólo un mes, ya realiza envíos a 45 países. Dos años después, recibe 50,000 visitas diarias. El comercio electrónico ya tiene a uno de sus grandes líderes.
- El primer Internet Explorer. Microsoft adquiere el código fuente de Mosaic y lanza su navegador oficial del sistema operativo Windows, en el que viene incluido. Las primeras versiones del Explorer no afectan al líder Netscape.
- Remates por la red. En San José California, Pierre Omidyar funda eBay con la intención de completar una colección de caramelos. Advierte que puede utilizar el sitio para que otras personas ofrezcan lo que ya no usan. Un puntero láser inservible es el primer artículo vendido. Su precio fue de U$S 14.83.
- Llega Altavista. Se lanza Altavista, un poderoso motor de búsqueda.

1996.

- El ciberespacio se Independiza. John Perry Barlow, poeta y antiguo letrista del grupo musical Grateful Dead, publica la Declaración de Independencia del Ciberespacio.
- Hotmail. Este primer servicio de e-mail basado en la web, más tarde pasará a pertenecer a Microsoft.
- Inician una segunda Internet. 34 universidades de EE.UU. se reúnen para definir los objetivos de Internet2: una red de alta velocidad, centrada en la comunicación académica que se mantiene al margen de la Internet "comercial". Diez años

después la red está formada por 200 universidades y medio centenar de empresas de tecnología.

1997.

- La guerra de los Navegadores. La fiesta de lanzamiento de la nueva versión 4.0 del Internet Explorer celebrada en San Francisco, se convierte en el momento más visible de la denominada Guerra de los Navegadores. Las potencias en conflicto son Explorer y Netscape. Ante el gigantesco logo de su rival, los empleados de Netscape se concentraron exhibiendo un cartel con la leyenda “Netscape 72, Microsoft 18”, aludiendo a sus respectivas porciones de mercado.
- Bienvenido, blog. En su sitio llamado Robot Wisdom, Jorn Barrer decide agrupar y publicar diariamente las cosas más interesantes que encuentra en la red. Aunque ya existían cosas parecidas. Barrer es el primero en denominarlo Weblog (“log” significa “diario”). Otros lo abreviarán “blog”. Blog es un sitio web periódicamente actualizado, que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente. Existen programas especiales para crearlos. El autor siempre conserva la libertad de mantener publicado lo que pretende.

1998. Google. Larry y Sergey Brin fundan Google Inc., la empresa creadora del mayor motor de búsqueda de Internet, en funciones desde apenas un par de años antes. El nombre proviene del término matemático Googol (un 1 seguido de 100 ceros), simboliza la inmensidad de datos que se pueden encontrar en la red.

1999.

- Abre sus puertas el primer banco virtual. El First Internet Bank of Indiana ofrece todos los servicios bancarios exclusivamente por la red. Otras entidades se sumarán más adelante.
- Ataca Melissa. Cien mil ordenadores se ven atacados por un nuevo y temible virus llamado Melissa. Se colapsan los servicios de email y las casillas de correo se abarrotan de enlaces a sitios pornográficos.
- Napster se hace Escuchar. Shawn Fanning, un estudiante recién ingresado en una universidad de Boston, envía a 30 amigos un programa creado por él mismo para compartir archivos musicales. En pocos días, diez mil jóvenes lo han bajado. El

programa fue objeto de enormes controversias y juicios en relación con los derechos de autor y de las productoras discográficas. ¿El nombre del Programa? Napster.

- Messenger golpea a la puerta. El programa de mensajería instantánea diseñado por Microsoft para sus sistemas Windows, comienza su extensa carrera. Tres meses después está a punto de ser reciclado por su escaso éxito. Sin embargo, una inesperada avalancha de usuarios lo vuelve a popularizar, desplazando a su famoso predecesor, el ICQ.
- Blogger. Una pequeña empresa de San Francisco, Pyra Labs, lanza este sistema de publicación de Blogs. Blogger ayudará fuertemente a popularizar este formato. En el 2003 es adquirido por Google.

2000. Apocalipsis, no. Desde hace meses se teme que el paso de la cifra 99 a la 00 en los calendarios internos de las computadoras conduzca al caos, al colapso mundial de los datos informáticos. Sin embargo, nada sucede. Las computadoras, Internet y el mundo siguen su curso.

2001. Nace la Wikipedia. Jimbo Wales, con la ayuda de Larry Sanger, inician el proyecto Wikipedia: una enciclopedia libre y políglota basada en la colaboración. Toda persona con acceso a Internet puede modificar la gran mayoría de los artículos. Llegará a convertirse en la enciclopedia más gigantesca de la historia. Para mediados de 2008 supera los diez millones de artículos en más de 250 idiomas. La palabra Wikipedia combina wiki (que significa “rápido” para los hawaianos) con paideia (educación en griego).

2003.

- El dominio de los Niños. Se crea el dominio “.kids” para denominar a los sitios seguros para los niños.
- Bajar música ya es legal. Apple Computer presenta Apple iTunes Music Store, que permite bajar legalmente temas musicales pagando 0.99 dólares por cada uno.
- Una segunda vida para todos. Nace Second Life, un mundo virtual en donde cualquier persona puede residir a través de su avatar o personaje. Esta segunda vida permite hacer todo lo que se da en la vida real, sin las limitaciones de ésta: amar, trabajar, crear objetos artísticos, edificar una casa y hasta ganar Linden

Dólares ($L), moneda intercambiable en el mundo físico. La idea, desarrollada por Linden Lab, resulta muy exitosa: decenas de miles de personas se mueven por su Second Life todos los días. Atraídos por el éxito de SecondLife, infinidad de empresas establecen negocios y publicidad en esta economía virtual. Algunos países incluso instalan embajadas.

2004.

- Facebook muestra la cara. Pensando en sus compañeros de Harvard, el estudiante Mark Zucherberg crea un sitio web de redes sociales. El nombre alude al folleto que reciben los recién ingresados, con fotos de sus compañeros para ayudar a identificarlos. Muy pronto rebasa el marco universitario. En el 2008 cuenta con cerca de 100 millones de usuarios activos. Facebook permite localizar a personas con quienes se ha perdido el contacto y hacer otros amigos para intercambiar mensajes, fotos y compartir un sinnúmero de actividades.
- Tienes un Gmail. - El nuevo servicio de e-mail de Google ofrece una gran capacidad de almacenamiento gratuito: 1 gigabyte.
- La web se hace Social. Se crea el término Web 2.0 para definir el uso de la www que busca aumentar la creatividad, el intercambio de información y la colaboración entre usuarios.
- ¿La Segunda Guerra? Se publica el Mozilla Firefox. En los primeros 99 días obtiene 25 millones de descargas. De esta manera se da origen a lo que algunos consideran la “Segunda Guerra de los Navegadores” entre el recién llegado, Internet Explorer y otros como Ópera y Safari.
- Se presenta Digg. Digg es un sitio web especializado en noticias sobre ciencia y tecnología, creado por Kevin rose, Jay Adilson y otros. Su control editorial es democrático, ya que depende de los votos de los usuarios. Los aportes se incorporan a la página principal una vez que han recibido una treintena de “diggs”, que para el caso se traduce como votos. Digg es otro de los sitios emblemáticos de la Web 2.0.

2005. Nos vemos en YouTubeChad. Hurley, Steve Chen y Jawed Karim fundan un sitio web que permite a los usuarios compartir videos digitales. La facilidad para alojar videos personales de hasta 10 minutos de duración lo hacen extremadamente popular

y a veces polémico. 1,650 millones de dólares convierten a YouTube en propiedad de Google en octubre de 2006. Un mes más tarde es considerado “El invento del Año” por la revista Time.

2006. Mil cien millones de usuarios. Las cifras del crecimiento de Internet no paran de sorprender. A esta altura se especula con que para el año 2015 habrá 2 mil millones de usuarios.

2007. El Iphone Apple lanza su teléfono celular capaz de conectarse a Internet.

4.2. Antecedentes Investigativos

En la actualidad existe una gran cantidad de grupos de investigación referentes a los temas principales que trata este documento. A continuación listamos algunos de los grupos de cuyo objeto de investigación son proyectos propios de la Ingeniería de Sistemas entre ellos la Seguridad Informática, firewalls y estándares de seguridad ISO 27001.

4.2.1. Contexto Internacional

A continuación presentamos algunos proyectos concernientes al tema a nivel internacional:

Según Bustamante (2010) este trabajo se busca describir y analizar los factores que intervienen en la seguridad en redes, a partir de los usuarios que buscan la mayor protección y confidencialidad de información en su red, utilizando herramientas y políticas de seguridad, para alcanzar ese fin. Pero para poder lograrlo se debe conocer contra quien debe protegerse y como son los medios en los que operan los atacantes, ya que con el paso de los años, las herramientas tanto de seguridad, como las herramientas para hackear, se van haciendo más potentes, destructivas y con una alta calidad. Y es importante saber en dónde está esa evolución en nuestra actualidad, para el cuidado de las redes.

Además para Mayo R (2006) auditar, de manera correcta, los mecanismos de seguridad utilizados en el ofrecimiento de los servicios de tecnologías de información (IT) es uno de los elementos fundamentales para el éxito de esta labor. El termino auditar correctamente incluye varios elementos importantes, uno de ellos es contar con un modelo de auditoria completo, equilibrado y técnicamente correcto. Este documento propone un modelo de auditoria de la seguridad informática para aquellos servicios IT que se ofrecen por RedULA para la universidad delos Andes, extensible para cualquier entidad de características similares.

Y Guachi, T (2012) nos dice que este proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Para Ferrer, M (2006) los usuarios de domicilios particulares y de las empresas disponen de un amplio abanico de comodidades que les permiten gestionar su trabajo a través de la pública de Internet. Esto puede suponer un problema si no se cumplen ciertas medidas de seguridad y de control para evitar las violaciones de datos que se irrumpen en la red.

La confidencialidad de los datos adquiere mayor importancia y dificultad de mantenimiento en el ámbito empresarial, donde la comunicación se establece entre la red privada de la empresa e Internet; así pues, este proyecto se enfoca concretamente en un escenario empresarial. Para garantizar un nivel de seguridad entre dos o más redes debe existir un sistema de aislamiento que evite comunicaciones indeseadas llamado Firewall. Por ello, este proyecto consiste en el estudio, la implementación y el análisis de tres tipos de Firewall sobre una Red Desmilitarizada o DMZ, en la cual se configuran los servicios más comunes que ofrece una empresa y que deberán ser protegidos por el Firewall para un acceso restringido.

4.2.2. Contexto Nacional

A nivel nacional existen grupos de investigación cuyos trabajos se encuentran publicados en las plataformas de Colciencias cvLac y grupLac. Algunos de sus trabajos a continuación:

Ladino, M (2011) nos muestra este artículo para una descripción de los fundamentos de la norma ISO 27001 y su aplicación en las organizaciones. Como caso práctico se presenta una experiencia de implementación de la norma en una organización, esta norma puede ser implantada en una empresa con el objetivo de obtener la certificación o simplemente como mejores prácticas para perfeccionar algunos aspectos de seguridad en la empresa. Adicionalmente se indica cómo implementar estas buenas prácticas en empresas pequeñas que no pueden realizar la certificación.

Para Guillen, E. (2011), la Telemedicina hace posible realizar de forma remota, varios procedimientos médicos y clínicos como: exámenes, diagnósticos y supervisión de tratamientos, utilizando recursos tele informáticos como computadores, servidores, equipos de procesamiento de imágenes, Internet y equipos de transmisión y recepción de información. La transmisión de la información de los pacientes crece día con día, vinculando otra serie de problemas relacionados con el tráfico y seguridad de los datos. En el tema de la seguridad, aún existe divergencia en los criterios de almacenamiento, acceso y transmisión de información de los pacientes porque los requerimientos físicos y lógicos varían para cada empresa, equipo desarrollador o intereses particulares. El presente trabajo hace un análisis respecto del tema de la seguridad informática sobre una red de Telemedicina. Incluye un análisis sobre los procedimientos de los servicios de Telemedicina más característicos y sus requerimientos de seguridad. Los requerimientos fueron estudiados y seleccionados a partir de los estándares internacionales regulatorios que se adapten a las necesidades básicas de seguridad de los servicios de Telemedicina.

Según Támara, G. (2006), se facilita una solución de seguridad de red personalizada de muy bajo costo para las pequeñas y medianas empresas, permitiéndoles identificar y afrontar con precisión los riesgos y tener una protección integral y completa. Se detectaron las necesidades que tienen las PYMES y se implementó un Servidor Firewall Linux. Básicamente se configura un host con la herramienta Iptables para definir la reglas de filtrado de paquetes según las políticas de seguridad establecidas para la protección del flujo de datos entre dos redes. Se hizo un análisis funcional al firewall, instalando servicios a los hosts de las redes locales para verificar la veracidad y factibilidad de las reglas configuradas, en el cual el comportamiento del firewall fue muy efectivo de acuerdo a las exigencias de las políticas de seguridad creadas.

Echeverry, J. (2009), en el trabajo se desarrolló al interior del Grupo de Investigación en Seguridad y Sistemas de Comunicaciones (GISSIC) del programa de Ingeniería en Telecomunicaciones de la Universidad Militar Nueva Granada, el cual está compuesto por los semilleros Enigma y Claude Shanon, para seguridad en comunicaciones y procesamiento de señales respectivamente, con el fin de desarrollar, implementar y proponer sistemas y metodologías para el desarrollo de los sistemas de seguridad y de comunicaciones con aplicabilidad local y globalizada. En conjunto con la División Informática de la Universidad Militar Nueva Granada, quienes están a cargo de los recursos informáticos dispuestos para los procesos académicos y administrativos y en gran parte, los directos responsables del sistema de información de la institución. El trabajo consiste en definir una metodología para diagnosticar el estado de la seguridad informática de la red de datos de la Universidad, de acuerdo con los resultados de ejecutar una evaluación del riesgo a la red de datos, lo que permite identificar cuáles son las áreas con mayor grado de criticidad y donde se debe hacer énfasis en el diagnóstico. El diagnóstico de la seguridad se lleva a cabo con la ejecución de unas tareas, que son realizadas con la utilización de aplicaciones de seguridad, en su gran mayoría software libre, y que a la vez quedan propuestas dentro de la metodología como una opción para ejecutar el diagnóstico.

4.2.3. Contexto Local

En el contexto local existe poca información disponible y la inexistencia de grupos de investigación en las principales universidades que se dediquen al tema en la ciudad de Montería. Solo contamos con un trabajo referencia en la Universidad de Córdoba.

Moreno, M. & López, C. (2013), nos dice que la empresa Nextin S.A.S presta servicios de Telefonía IP, desarrollo y producción de software, está ubicada en la ciudad Montería, departamento de Córdoba, con poco tiempo en el mercado, en la cual en sus gestiones diarias se ha venido presentando acceso indebido de páginas web, uso desmedido de recursos de ancho de banda, fallas en calidad del servicio, entre otras. Este proyecto se centra en el analizar y diseñar de políticas de seguridad en pequeñas y medianas empresas (PYMES) puntualmente en la empresa Nextin S.A.S, para con ello proteger y gestionar la información de una manera más confiable, con este fin se hace un estudio en el área urbana de la ciudad de Montería para determinar cómo es el estado actual de las organizaciones en cuestión de herramienta, fallas, prácticas y políticas de seguridad de la información, dicho estudio nos mostrara un panorama general de las fallas o vulnerabilidades para así tomar medidas y controles en la empresa de nuestro caso de estudio.

4.3. Sistema Gestión de Seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende:

- La política.
- La estructura organizativa.
- Los procedimientos.
- Los procesos y
- Los recursos necesarios

Para implantar la gestión de la seguridad de la información. Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente. Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello.

Un SGSI contiene en primer lugar, las pautas que se van a seguir en la organización para garantizarla seguridad de la información y las responsabilidades de cada cual al respecto. El SGSI recoge los objetivos que se pretenden obtener y los medios con que se va a contar para ello.

Para determinar ambas cosas, se realiza un análisis de riesgos que da la medida de hasta qué punto los activos están expuestos a que les ocurran fallos de seguridad y cuál sería el impacto en caso de que lleguen a ocurrir. Con esa información se establece el punto de partida, cual es el estado en el que está la seguridad y se decide cual se pretende conseguir, así como cuál es el objetivo para un periodo de tiempo determinado. A partir de ahí, se deciden las acciones a tomar para reducir esos riesgos al nivel que se decidido que sea el objetivo.

Las acciones que se tomen deben documentarse dentro del SGSI, mediante procedimientos y planes para su ejecución.

Por tanto definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

4.3.1. Consideraciones Generales

Seguridad Informática: Son los mecanismos utilizados para asegurar la información a través de los recursos tecnológicos de una red:

- Hardware.
- Software.
- Aplicaciones.

Seguridad de la Información: Son todos aquellos mecanismos utilizados para proteger los datos (confidencialidad, integridad y disponibilidad).

Seguridad de las Comunicaciones: Mecanismos para proteger el transporte de la información, como por ejemplo:

- VPN.
- SSL.
- SSH.
- Canales dedicados.

Seguridad Física: Son todos los mecanismos físicos utilizados para proteger las áreas de organizaciones, por ejemplo:

- Vigilancia.
- Sensores.
- Control de acceso por biométrico.
- CCTV (Circuito Cerrado de Televisión).

Seguridad Computacional: Es un conjunto de mecanismos lógicos que se implementan con el fin de proteger la información.

Ilustración 1. Área de Protección

Vulnerabilidad: Es la debilidad que presenta un sistema, por ejemplo puertos abiertos que no estén configurados, es decir, la debilidad no está en tener puertos abiertos sino en no configurarlos correctamente.

Debilidad: Pérdida parcial o total de un control.

Amenazas: Materialización de la debilidad, es decir, todo lo que puede pasar si es explotada la debilidad.

Tipos de amenazas:

- Naturales (incendios, terremotos, etc.)
- Políticas/sociales (disturbios, huelgas, etc.)
- Físicas (Fallas energéticas, de hardware, etc.)
- Humanas (Intencionales, no intencionales)
- Intencionales: Destrucción física, virus, Espionaje, robo de información, entre otros

Riesgo: Probabilidad de que una debilidad, amenaza e impacto, afecte el negocio de la organización.

Control: Mecanismo que reduce las debilidades o las amenazas de un sistema. Los tipos de control son: preventivos, correctivos y detectivos.

Los preventivos previene problemas antes de que sucedan, los detectivos son Controles que detectan errores maliciosos y los correctivos minimizan el impacto de una amenaza, corrigen problemas detectados.

4.3.2. Ciclo de vida de la seguridad

El ciclo de vida de la seguridad, funciona como cualquier otro ciclo, es decir, con una retroalimentación continua.

Ilustración 2. Ciclo de Vida de la Seguridad

Diagnóstico: Consiste en determinar el estado del nivel de seguridad de la organización. Para realizar este proceso se deben seguir los siguientes pasos:

Levantamiento de información Este proceso se realiza teniendo en cuenta los siguientes ítems:

Tecnología: Infraestructura física, topología de la red, información de las plataformas de los servidores, elementos de seguridad, equipos activos, aplicaciones, canales de comunicación, etc.

Procesos: A nivel de procesos es importante conocer el ciclo:

Entradas-Procesos-Salidas

Personas: Roles, costumbres.

El proceso de levantamiento de la información. Para empezar a conocer la información de un servidor interesan los siguientes datos:

- Nombre del servidor.
- Función.
- Dirección IP.
- Sistema operativo.
- Actualizaciones.
- Administrador.

Todos estos datos deben ser consignados en una tabla. Ahora si me interesará conocer la información de un equipo activo, debo tener en cuenta los siguientes datos:

- Nombre.
- Dirección IP.
- Tipo de administrador (remoto o local).
- Versión de software.
- Actualizaciones.
- Marca.
- Función.
- Nombre del administrador.

Estos datos deben estar consignados en una tabla.

Para obtener la información acerca de la topología de la red, obtengo los siguientes datos:

- Topología física
- Topología lógica

Para obtener información acerca de la infraestructura física, obtengo la siguiente información:

- Espacios.
- Controles de acceso.
- Tipo de cableado.
- Control de fallas físicas.

Para obtener información acerca de los canales de comunicación:

- Tipo de enlace (Alámbrico o inalámbrico)

Análisis de la información: La información se analiza con el fin de identificar cuáles son las vulnerabilidades.

Identificación de vulnerabilidades: Para realizar el proceso de identificación de vulnerabilidades se deben seguir los siguientes pasos:

- Metodología de Ethical Hacking.
- Identificación de vulnerabilidades administrativas (lista de chequeo) mediante Norma 27001.

Análisis de riesgos

El análisis de riesgos se puede realizar mediante los siguientes métodos:

- Métodos cualitativos.
- Métodos cuantitativos.
- Riesgos altos, medios y bajos.

Panorama de riesgos: Se debe identificar que es cada riesgo, es decir, a cuanto equivalen los riesgos altos, los riesgos medios y los riesgos bajos.

Diseño: El diseño de seguridad parte de las políticas, normas y estándares y/o procedimientos (Norma 27001), en esta parte se desarrollan las siguientes características:

Arquitectura de seguridad:

Infraestructura de seguridad

- Arquitectura de Firewall
- Arquitectura de IDS/IPS
- Arquitectura de VPN

Cifrado de información

- Certificados digitales.
- Firmas digitales.
- Cifrado de información.

Implementación del Modelo: La implementación del modelo abarca los siguientes ítems:

- Creación de políticas.
- Creación de normas (las normas son los pasos para cumplir con una política).
- Creación de estándares (un estándar es un modelo de mejores prácticas).
- Creación de procedimientos.
- Implementación de arquitectura tecnológica (método de defensa en profundidad).
- Planes de continuidad.
- Capacitación (seguridad).

Monitoreo

- Administración de logs.
- Gestión de incidentes de seguridad.

- Control de cambios.
- Detectores de intrusos (IDS/IPS).

Es necesario decir que los incidentes de seguridad se presentan en tres fases: el antes, el durante y el después.

El antes se refiere a la administración de logs, es decir, ver que sucedió; el durante se refiere a la gestión del incidente y el después se refiere a toda la parte de computación forense.

Hacking Ético: Los aspectos a tratar en esta parte de ethical hacking (Hacking Ético) se tratan a un nivel en el cual única y exclusivamente nos interesa conocer las debilidades de una organización de forma NO INTRUSIVA.

Este es el punto de partida para detectar las vulnerabilidades en los sistemas de información con el fin de corregir dichas vulnerabilidades.

Los métodos de acceso tratados aquí pueden ser de tipo intrusivo o de tipo no intrusivo, como lo mencionamos anteriormente, nosotros nos concentraremos en los métodos no intrusivos.

Los intrusivos suceden cuando al momento de encontrar una debilidad en el sistema de información.

Otro caso de intrusión sucede cuando encuentro una vulnerabilidad e informo a la organización que voy a hacer las pruebas de intrusión, luego de realizar la intrusión, reporto todas las fallas (hacking ético intrusivo).

Los no intrusivos: Suceden cuando encuentro las vulnerabilidades, pero no ingreso a sus sistemas, solo lo reporto (hacking ético no intrusivo).

Es necesario conocer diferentes términos que se relacionan con el ethical hacking, así que empezaremos a nombrarlos:

Hacker: Una persona que se dedica a buscar vulnerabilidades y explotarlas; por ejemplo, un hacker encuentra debilidades en una página web y cambia su contenido, es decir, explota su vulnerabilidad.

Cracker: Es un hacker que tiene fines lucrativos en su accionar.

Trasher: Personas que se dedican a buscar información o contraseñas de acceso en las papeleras de reciclaje.

Lammer: Se dedican a probar herramientas de hacking.

Piratas Informáticos: Se dedican a copiar, distribuir y utilizar software ilegalmente.

Metodología Ethical Hacking: Para iniciar la metodología de ethical hacking lo primero que se debe hacer es identificar cuales servicios presta la empresa, los cuales pueden ser:

- Servicios de red interna.
- Servicios hacia internet.

4.3.3. Marco Legal

Ley 1341 del 2009

Objeto: Determina el marco general para la formulación de las políticas públicas que regirán el sector de las tecnologías de la información y las comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y el espectro radioeléctrico, así como las potestades del estado en relación con la planeación, la

gestión, la administración adecuada y eficiente de los recursos, regulación, control, y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes en el territorio nacional a la sociedad de la información.

Decreto 1900 de 1990

Objeto: El presente decreto tiene como objeto el ordenamiento general de las telecomunicaciones y de las potestades del estado en relación con su planeación, regulación y control, así como el régimen de derechos y deberes de los operadores y de los usuarios.

Norma ISO/IEC 27001 tecnología de la información - técnicas de seguridad - código para la práctica de la gestión de la seguridad de la información.

Esta norma proporciona una guía a través de 11 dominios de seguridad para gestionar el sistema de la seguridad de la información de una organización independientemente del tamaño o servicios que ésta ofrezca, ya que esta norma contempla todos los controles posibles para salvaguardar la información de una organización.

4.4. Políticas de Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4.5. Norma ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen:

ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.

ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.

ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.

ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de

seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.

ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

ISO/IEC 27007 - Es una guía para auditar al SGSI. Se encuentra en preparación.

ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades

4.6. Firewall

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

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

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

También es frecuente conectar los cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

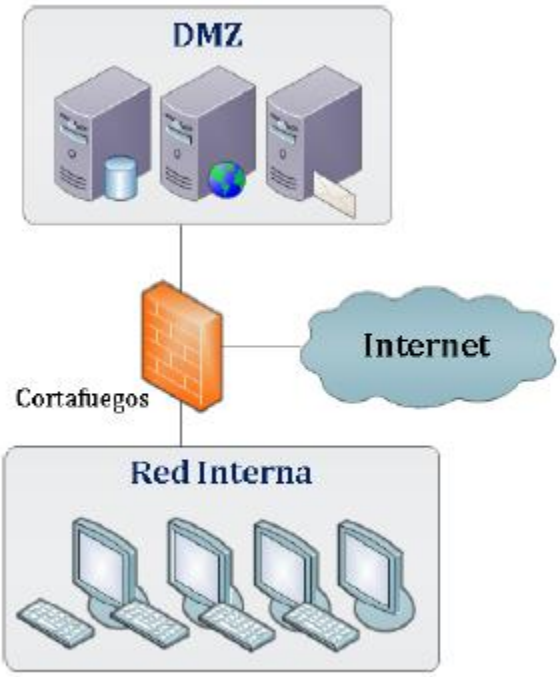

Ilustración 3. Firewall

4.7. Sistema de Detección de Intrusos IDS

Un sistema de detección de intrusiones (o IDS de sus siglas en inglés Intrusión Detection System) es un programa de detección de accesos no autorizados a un computador o a una red.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS no detecta, gracias a dichos sensores, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al no entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como no puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

Existen dos tipos de sistemas de detección de intrusos:

HIDS (HostIDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.

NIDS (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

4.8. Sistema de Prevención de Intrusos IPS

Un Sistema de Prevención de Intrusos o Intrusion Prevention System ("IPS" en sus siglas en inglés), es un dispositivo de seguridad de red que monitorea el tráfico de red y/o las actividades de un sistema, en busca de actividad maliciosa. Entre sus principales funciones, se encuentran no sólo la de identificar la actividad maliciosa, sino la de intentar detener esta actividad. Siendo ésta última una característica que distingue a este tipo de dispositivos de los llamados Sistemas de Detección de Intrusos o Intrusion Detection Systems ("IDS" en sus siglas en inglés).

Entre otras funciones (como en el caso del IDS) se tiene que puede alertar al administrador ante la detección de intrusiones o actividad maliciosa, mientras que es exclusivo de un Sistema de Prevención de Intrusos (IPS) establecer políticas de seguridad para proteger al equipo o a la red de un ataque.

De ahí que se diga que un IPS protege a una red o equipo de manera proactiva mientras que un IDS lo hace de manera reactiva.

Otras funciones importantes de estos dispositivos de red, son las de grabar información histórica de esta actividad y generar reportes.

Los IPS se clasifican en cuatro diferentes tipos:

- Basados en Red Lan (NIPS): monitorean la red lan en busca de tráfico de red sospechoso al analizar la actividad por protocolo de comunicación lan.
- Basados en Red Wireless (WIPS): monitorean la red inalámbrica en busca de tráfico sospechoso al analizar la actividad por protocolo de comunicación inalámbrico.

- Análisis de comportamiento de red (NBA): Examina el tráfico de red para identifica amenazas que generan tráfico inusual, como ataques de denegación de servicio ciertas formas de malware y violaciones a políticas de red.
- Basados en Host (HIPS): Se efectúa mediante la instalación de paquetes de software que monitorean un host único en busca de actividad sospechosa

Los IPS categorizan la forma en que detectan el tráfico malicioso:

- Detección basada en firmas: como lo hace un antivirus.
- Detección basada en políticas: el IPS requiere que se declaren muy específicamente las políticas de seguridad.
- Detección basada en anomalías: en función con el patrón de comportamiento normal de tráfico.

4.9. Proxy

Según Wikipedia “Un proxy, o servidor proxy, en una red informática, es un servidor (un programa o sistema informático), que sirve de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, mejorar el rendimiento, mantener el anonimato, proporcionar Caché web, etc; este último sirve para acelerar y mejorar la experiencia del usuario mediante permisos que guardará la web, esto se debe a que la próxima vez que se visiten las páginas web no se extraerá información de la web si no que se recuperara información de la caché.

La palabra inglesa proxy significa procurador en español.

El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

De ellos, el más famoso es el servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.

También existen proxy para otros protocolos, como el proxy de FTP.

El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Un componente hardware también puede actuar como intermediario para otros.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo que la solicitó.

Hay dos tipos de proxys atendiendo a quien es el que quiere implementar la política del proxy:

Proxy local: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).

Proxy externo: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

5. CAPITULO I. ANALISIS DEL RIESGO EXISTENTE EN LA RED DE DATOS DE LA E.S.E. HOSPITAL SAN NICOLÁS.

Este capítulo comprende la recolección de información para mostrar el estado actual del hospital, así como también el análisis de riesgo que se llevó acabo en el Hospital San Nicolás, teniendo en cuenta su situación actual, este análisis fue realizado con la herramienta de MSAT 4.0 de Microsoft, por ser esta herramienta una de las más utilizadas y valoradas en el mercado por su alta experiencia en compañías y su base en la norma ISO/IEC 27001.

5.1. Inventario de Activos

Es muy importante conocer los equipos tecnológicos con que cuenta la empresa en los cuales se gestiona y viaja la información, adicional a eso conocer la topología y el direccionamiento de la red de datos.

Tabla de Inventario General de Activos

Tipo de Equipo	Cantidad
Modem ADSL	1
Router WIFI	1
Switch	4
Servidores	3
Computadores	50
DVR	1
Cámaras análogas	16
Teléfonos Volp	30

Tabla 1. Inventario General de Activos

Tabla de Inventario detallado de Activos

Equipo	Características	No. de Equipos	Departamento al que pertenece
PC Clon	Windows 7, memoria 2Gb, impresora Hp LaserJet P1102w. Ofimática, antivirus kaspersky, con conexión red, monitor LCD 17", no tiene tarjeta de red y procesador celeron 2.4.	2	Auditoria
PC Clon	Windows 7, memoria 2Gb, office 2010, no tiene antivirus, con conexión red, monitor LCD 22" y teléfono.		
PC Clon	Windows 7, memoria 2Gb, no tiene impresora, ofimática (office 2010 original), antivirus avira, con conexión red,	4	Cartera

	monitor LCD 22", no tiene tarjeta de red, procesador celeron 1.7 y no tiene teléfono.		
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet2050, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 19", procesador celeron 2.4 y no tiene teléfono.		
PC Clon	Windows 7, memoria 2Gb, impresora HP LaserJet P1102w, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 19", procesador celeron 2.4 y teléfono. Observación: Se reinicia PC		
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet2050, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 19", procesador celeron 2.4		
PC Clon	Windows 7, memoria 4Gb, impresora multifuncional Samsung SCX-3200, ofimática (office 2010 original), antivirus essencial, con conexión red, monitor LCD 17", procesador celeron 2.4 y teléfono.	1	Apoyo Presupuestal
PC Clon	Windows 7, memoria 1Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 21", procesador celeron 2.4 y teléfono. Observación: Se reinicia, demora la impresión y línea de tel. aparte.	2	Pagaduría
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet2050, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 19", procesador celeron 2.4		
PC Clon	Windows 7, memoria 1Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), antivirus avast free, con conexión red, monitor LCD 17" y procesador celeron 2.4 y teléfono. Observación: Cambiar batería.	2	Jurídica
PC Clon	Windows 7, memoria 2Gb, ofimática (office 2010 original), no tiene antivirus, con conexión red, monitor LCD 19", procesador celeron 2.4		
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), antivirus Eset NOD32, con conexión red, monitor LCD 19" y procesador celeron 2.4 y teléfono. Observación: Equipo se reinicia	1	Recurso humano
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRA, monitor LCD 19" y procesador celeron 2.4, teléfono y tarjeta de red quemada.	1	Pediatría
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet D1560, ofimática (office 2010 original), no tiene antivirus, monitor LCD 19" y procesador Pentium dual core 2.8, teléfono y tarjeta de red.	2	SIAU
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet D1560, ofimática (office 2010 original), no tiene antivirus, monitor		

	LCD 19" y procesador Pentium dual core 2.8, teléfono y tarjeta de red		
PC Clon	Windows 7, memoria 2Gb, impresora EPSON L355, ofimática (office 2010 original), no tiene antivirus, monitor LCD 17" y procesador Pentium dual core 2.6, Tel. voip compartido y tarjeta de red.	3	Estadísticas
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet laser p1102w, ofimática (office 2007 original), antivirus AVIRAfree, monitor LCD 21" y procesador celeron 2.6, Tel. voip y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora EPSON L355, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet2050, ofimática (office 2007 original), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.5, UPS y tarjeta de red.	1	Vacunación
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red. Observación: Esta oficina se encuentra un pack con las siguientes características 2 switch 3 com 2 patch panel 1 regulador de voltaje de cámaras de seguridad 12v Ningún punto de red esta rotulado	1	Facturación-Vacunación
PC Clon	Windows 7, memoria 2Gb, impresora HP deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.	6	Facturación
PC Clon	Windows 7, memoria 2Gb, impresora compartida, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.4, UPS y tarjeta de red. Observación: Hay dos equipos en desuso falta CPU y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador Core 2 duo 2,8GHZ, UPS y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora compartida, ofimática (office 2007 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red. Observación: Se hizo configuración en urgencia star enfermera se encuentra desconfigurada.		
PC Clon	Windows 7, memoria 2Gb, impresora compartida, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.4, UPS y tarjeta de red. Observación: Hay dos equipos en desuso falta CPU.		

PC Clon	Windows 7, memoria 2Gb, impresora compartida, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.4, UPS y tarjeta de red. Observación: Hay dos equipos en desuso falta CPU y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2007 original), antivirus AVIRAfree, monitor LCD 17", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red	1	Maternidad
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2007 original), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red	1	Urgencia
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red	1	Almacén
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2010 original), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red. Observación: Equipo se reinicia	4	Odontología
PC Clon	Windows 7, memoria 4Gb, impresora Hp deskjet laser p1102w, ofimática (office 2010 original), antivirus no tiene, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red. Observación: Equipos con virus acceso directo.		
PC Clon	Windows 7, memoria 4Gb, impresora compartida, ofimática (office 2010 original), antivirus no tiene, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.		
PC Clon	Windows 7, memoria 4Gb, impresora compartida, ofimática (office 2010 original), antivirus no tiene, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.		
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (office 2010 original), antivirus no tiene, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.	1	Citología
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (open office 3.2), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.5, UPS y tarjeta de red. Nota: todos con las mismas características y funcionando.	14	Consultorios
PC Clon	Windows 7, memoria 2Gb, impresora Hp deskjet laser p1102w, ofimática (2007), antivirus AVIRAfree, monitor LCD 21", Tel. voip, procesador celeron 2.6, UPS y tarjeta de red.	1	Crecimiento y desarrollo
PC Clon	Windows 7, memoria 4Gb, impresora Hp deskjet laser p1102w, ofimática (2007), antivirus McAfee security, monitor LCD 21", Tel. voip, procesador Pentium dual 2.5, no UPS	1	Hipertensión arterial

Tabla 2. Inventario detallado de Activos

El direccionamiento que se está utilizando es de un solo segmento de red. A saber: 192.168.1.0/24 y una topología de red en estrella.

5.2. Esquema de la red de datos del Hospital San Nicolás de Planeta Rica.

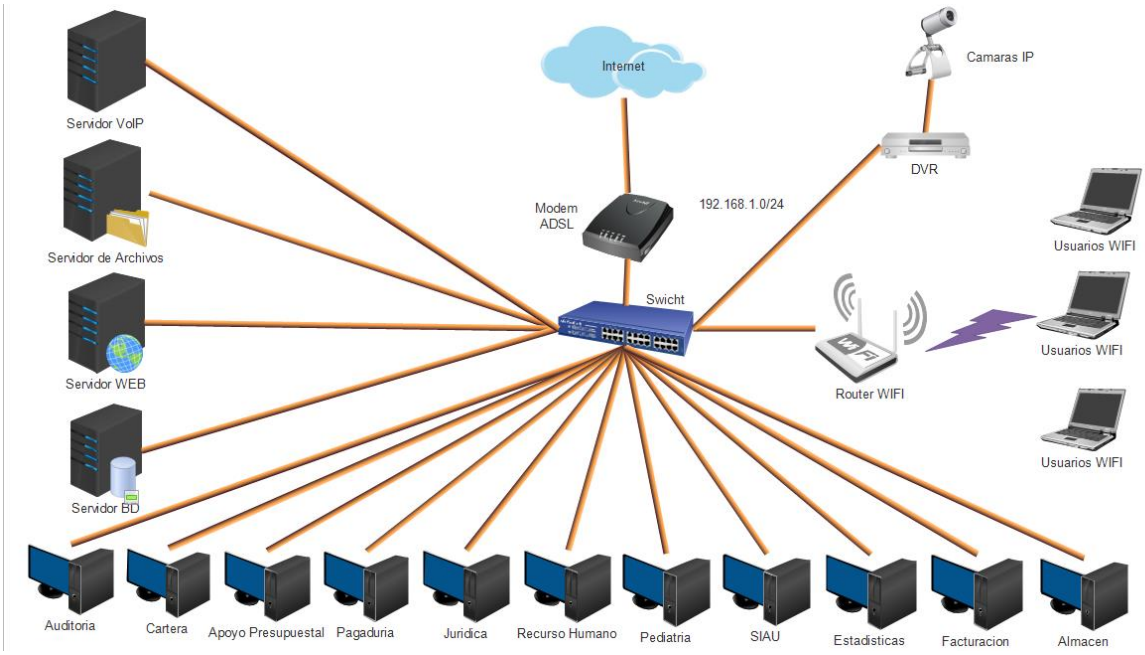

Ilustración 4. Red de datos Hospital San Nicolás de Planeta rica

5.3. Análisis de Riesgo

5.3.1. Análisis de la situación

Este gráfico de la sección representa los conceptos de la empresa descritos anteriormente y se basa en las respuestas que proporcionó. Recuerde:

- BRP (Perfil de riesgos de negocio) es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa
- DiDI (Defense-in-Depth index) es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa.

- La madurez de la seguridad es una medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

Resultados:

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Tabla de Áreas de Análisis MSAT

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Infraestructura	●	●
Aplicaciones	●	●
Operaciones	●	●
Personal	●	●

Tabla 3. Áreas de Análisis MSAT

5.3.2. Risk-Defense

Este gráfico, dividido en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad.

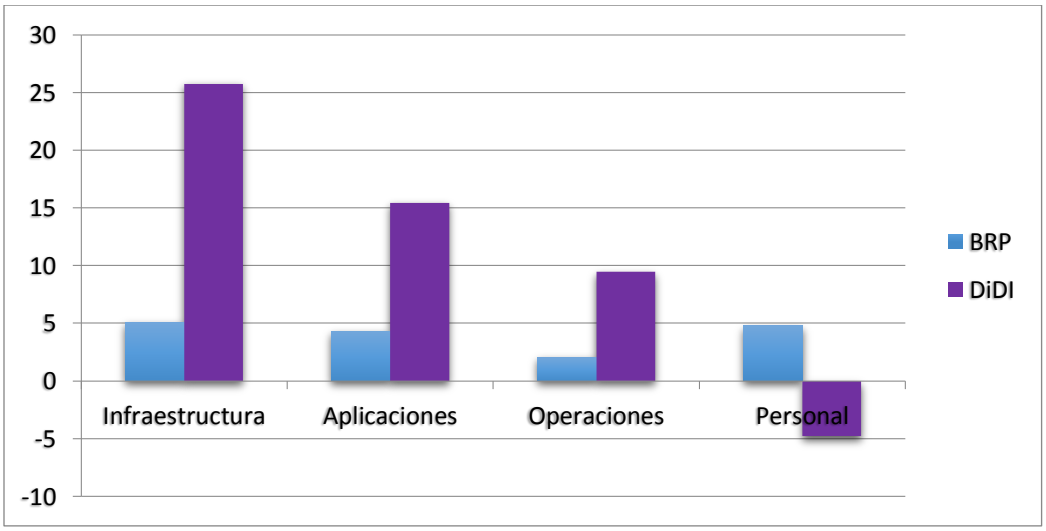

Ilustración 5. Risk-Defense

Por lo general, es mejor contar con una calificación de DiDI del mismo nivel que otra de BRP para la misma categoría. Un desequilibrio, ya sea dentro de una categoría o

entre categorías, en cualquier dirección, puede indicar la necesidad de volver a alinear sus inversiones de TI.

5.3.3. Madurez de la seguridad

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa. No todas las empresas deben esforzarse por alcanzar el nivel óptimo, pero todas deben evaluar en qué punto se encuentran y determinar el lugar que deberían ocupar en vista de los riesgos comerciales a los que se enfrentan. Por ejemplo, puede que una empresa con un entorno de bajo riesgo no necesite nunca subir encima del límite superior del nivel básico o el límite inferior del nivel estándar. Las empresas con un entorno de alto riesgo probablemente entren de lleno en el nivel optimizado. Los resultados del perfil de riesgos para la empresa le permiten hacer un balance de los riesgos.

Tabla de la Madurez de la seguridad

Madurez de la seguridad	Una medida de las prácticas de una empresa con respecto a las mejores prácticas de la industria para la seguridad sostenible. Todas las empresas deben esforzarse en alinear su nivel de madurez y estrategia de seguridad asociada, en relación a los riesgos que conlleva su actividad comercial:
Básica	Algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva
Estándar	Capas múltiples de defensa utilizadas para respaldar una estrategia definida
Optimizada	Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas

Tabla 4. Madurez de la seguridad

5.3.4. Tarjeta de puntuación

De acuerdo con sus respuestas acerca de la evaluación de riesgos, sus medidas de defensa se han calificado de la siguiente forma. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Tabla de Tarjeta de Puntuación

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
ntivirus	●
Antivirus- Equipos de escritorio	●
Antivirus - Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso rem to	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●
Aplicaciones	●
Imple entación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●
Vulnerabilid des	●
Diseño de aplicaciones	●
Autenticación	●
Directivas de contraseñas	●

Operaciones	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configur ción	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●
Personal	●
R quisitos y evalua iones	●
Requisitos de seguridad	●
Evaluaciones de segur dad	●
Directiva y procedimientos	●
Comprobaciones del historial personal	●
Directiva de recursos humanos	●
Relaciones con terceros	●
Formación y conocimiento	●
Conocimiento e seguridad	●
Formación sobre seguridad	●

Autorización y control de acceso	●
Registro	●
Validación de datos de entrada	●
Metodologías de desarrollo de seguridad de software	●
Almacenamiento y comunicaciones de dato	●
Cifrado	●
Cifrado- Algoritmo	●

Tabla 5.Tarjeta de Puntuación

5.3.5. Iniciativas de seguridad

Las siguientes áreas no cumplen las mejores prácticas recomendadas y deben dirigirse a aumentar la seguridad de su entorno. Las secciones detalles de la evaluación y lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Tabla de Iniciativas de Seguridad

Prioridad alta	Prioridad intermedia	Prioridad baja
• Inalámbrico • Acceso remoto • Relaciones con terceros • Aplicación y recuperación de datos • Usuarios de acceso remoto	• Seguridad física • Antivirus • Cuentas inactivas • Desarrollado internamente	• Antivirus - Equipos de escritorio • Antivirus - Servidores • Autorización y control de acceso

Tabla 6. Iniciativas de Seguridad

5.3.6. Evaluación detallada

Esta sección del informe ofrece los resultados detallados para cada categoría, así como las mejores prácticas, recomendaciones y referencias de información adicional. Las recomendaciones son prioritarias en la siguiente sección.

5.3.6.1. Áreas de análisis

La siguiente tabla enumera las áreas incluidas para el análisis de alto nivel de esta evaluación de riesgos para la seguridad y explica la relación entre cada área y la seguridad. La sección "Detalles de la evaluación" describe los niveles de seguridad de su empresa (según las respuestas aportadas en la evaluación) con respecto a cada una de estas áreas. Asimismo, indica las prácticas más reconocidas del sector, además de ofrecerle recomendaciones para implantar tales prácticas.

Tabla de Áreas de análisis

Categoría	Importancia para la seguridad
Perfil de riesgos para la empresa (BRP)	
Perfil de riesgos para la empresa (BRP)	Comprender como la propia naturaleza de la empresa afecta a los riesgos es importante a la hora de decidir dónde aplicar los recursos que ayuden a paliar tales riesgos. El reconocimiento de las áreas le permitirá optimizar la asignación del presupuesto de seguridad.
Infraestructura	
Defensa del perímetro	La defensa del perímetro trata la seguridad del perímetro de la red, donde su red interna conecta con el exterior. Este es su primer escudo protector contra los intrusos.
Autenticación	Los procedimientos estrictos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos.
Gestión y control	La gestión, supervisión y el registro adecuados son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.
Aplicaciones	
Implantación y utilización	Cuando se implantan aplicaciones críticas para la empresa, hay que asegurar la seguridad y la disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse de que los errores de seguridad se corrigen y que no se introducen nuevas vulnerabilidades en el entorno.
Diseño de aplicaciones	Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial.
Almacenamiento y comunicaciones de datos	La integridad y confidencialidad de los datos son dos de las prioridades que debe garantizar cualquier empresa. La pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de una entidad como a su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos

	críticos.
Operaciones	
Entorno	La seguridad de una empresa depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. Pueden aumentar la seguridad incluyendo más que meras defensas tecnológicas. La capacidad del equipo de operaciones para mantener la seguridad del entorno depende de forma crucial de la documentación exacta del entorno y de las pautas.
Directiva de seguridad	La política de seguridad corporativa hace referencia a las directivas y a pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos de la empresa. Esta área incluye las directivas para todos los aspectos de la seguridad, como los usuarios, los sistemas y los datos.
Gestión de actualizaciones y revisiones	La gestión adecuada de actualizaciones y revisiones es un factor importante para la seguridad del entorno informático de las empresas. La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque.
Copias de seguridad y recuperación	Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallo de hardware o de software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad.
Personal	
Requisitos y evaluaciones	Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. Las evaluaciones periódicas realizadas por terceros independientes pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras.
Directivas y procedimientos	Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos.
Formación y conocimiento	Los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan a sus actividades diarias, para que no expongan a la empresa a mayores riegos de forma inadvertida.

Tabla 7. Áreas de análisis

5.3.7. Análisis de la evaluación

Esta sección está dividida en las cuatro principales áreas de análisis: infraestructura, aplicaciones, operaciones y personal.

5.3.7.1. Infraestructura

La seguridad de las infraestructuras se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que se deben implantar, cómo se crean y utilizan los hosts y la gestión y el mantenimiento de la red. La seguridad de la infraestructura efectiva puede ayudarle a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. Al establecer un diseño de la infraestructura que todos puedan comprender y seguir, podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar el riesgo para la infraestructura enfocándose en las áreas de seguridad de infraestructura que siguen:

- Defensa del perímetro—cortafuegos, antivirus, acceso remoto, segmentación
- Autentificación—directivas de contraseñas
- Gestión y control—hosts de gestión, archivos de registro
- Estación de trabajo—configuración de creación

Tabla de Infraestructura

Defensa del perímetro		
Subcategoría	**Mejores prácticas recomendadas**	
Reglas y filtros de cortafuegos	Los firewalls son un mecanismo de primera línea de defensa y se deben colocar en todas las ubicaciones de borde de red. Las reglas implementadas en los firewalls deben ser muy restrictivas y establecerse host a host y servicio a servicio. Al crear reglas de firewall y listas de control de acceso (ACL) de enrutador, céntrese primero en la protección de los dispositivos de control y de la red frente a ataques. El firewall debe estar establecido con una posición de denegación predeterminada, permitiendo únicamente el tráfico necesario. * Aplique el flujo de datos utilizando las ACL de red y las reglas de firewall. * Pruebe las reglas de firewall y ACL de enrutador para determinar si las reglas existentes contribuyen a ataques de denegación de servicio (DoS). * Implemente una o más DMZ como parte de una implementación de firewall sistemática y formal. * Coloque ahí todos los servidores accesibles a través de Internet. Restrinja la conectividad hacia las DMZ y desde ellas.	
	Resultados	**Recomendaciones**
Reglas y filtros de cortafuegos	Sus respuestas indican que no hay cortafuegos ni otros controles de acceso de nivel de red en el perímetro de la misma. Los cortafuegos son la	Utilice inmediatamente un cortafuegos (u otro dispositivo para controlar el acceso al nivel de la red) para proteger los recursos corporativos en el perímetro. El cortafuego

	primera línea de defensa, de ahí que resulten imprescindibles para proteger la red de los intrusos.	debe mantener una configuración predeterminada de negación a fin de permitir sólo el tráfico necesario para que el sitio funcione. Se deben usar filtros de entrada y de salida para evitar el acceso no autorizado a los servicios. Analice las reglas de los cortafuegos con regularidad para adaptarlas a los cambios en los servicios o las aplicaciones.
Reglas y filtros de cortafuegos	Sus respuestas indican que no utiliza software de cortafuegos basados en hosts para proteger los servidores.	Como una capa adicional de defensa, considere instalar cortafuegos basados en host en todos los servidores y piense también en emplear este software en todos los equipos de escritorio y portátiles en la empresa.
Reglas y filtros de cortafuegos	Sus respuestas indican que el cortafuego no se comprueba regularmente para asegurarse de que funciona correctamente.	Establezca pruebas periódicas del cortafuego. Asegúrese de que la funcionalidad responde según lo previsto, no únicamente desde el tráfico externo, y compruebe que el cortafuego también está respondiendo al tráfico interno.
Subcategories	**Mejores prácticas recomendadas**	
Antivirus	Implemente soluciones antivirus en todo el entorno en el nivel de servidor y de escritorio. Implemente soluciones antivirus especializadas para tareas específicas, como exploradores de servidores de archivos, herramientas de filtrado de contenido y exploradores de carga y descarga de datos. Configure soluciones antivirus para buscar virus en el entorno tanto de entrada como de salida. Las soluciones antivirus se deben implementar primero en servidores de archivos críticos y, a continuación, en servidores de correo, bases de datos y web. La solución antivirus se debe incluir en el entorno de generación predeterminado para escritorios y portátiles. Si utiliza Microsoft Exchange, utilice las capacidades de antivirus y filtrado de contenido adicionales en el nivel de buzón.	
	Resultados	**Recomendaciones**
Antivirus	Sus respuestas indican que no hay ningún software antivirus instalado en los servidores de correo electrónico.	Instale el software antivirus en todos los equipos del entorno corporativo.
Antivirus	Sus respuestas indican que no hay ningún software antivirus instalado en los hosts del perímetro de red.	Instale el software antivirus en todos los equipos del entorno corporativo.
Subcategoría	**Mejores prácticas recomendadas**	
Antivirus - Equipos de escritorio		
	Resultados	**Recomendaciones**
Antivirus - Equipos de escritorio	Su respuesta indica que los equipos de escritorio utilizan soluciones antivirus.	Continúe con la práctica. Utilice una directiva que requiera a los usuarios a actualizar las firmas de virus. Piense en añadir el cliente antivirus al entorno predeterminado de creación de estaciones de trabajo.
Subcategoría	**Mejores prácticas recomendadas**	

Antivirus - Servidores		
	Resultados	**Recomendaciones**
Antivirus - Servidores	Sus respuestas indican que ha utilizado soluciones antivirus en el nivel del servidor.	Continúe con la práctica. Plantéese controlar activamente los clientes antivirus de los servidores desde una consola de gestión central para la utilización de configuraciones y firmas de virus. Si utiliza Microsoft Exchange, considere emplear las funciones adicionales de antivirus y los filtros de contenidos para los buzones de correo.
Subcategoría	**Mejores prácticas recomendadas**	
Acceso remoto	Es importante seguir un proceso de creación de informes de incidentes y repuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.	
	Resultados	**Recomendaciones**
Acceso remoto	Sus respuestas indican que existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro.	Utilice VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH. Utilice conectividad sitio-a-sitio basada en la tecnología IPSec. Configure listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.
Acceso remoto	Sus respuestas indican que existen empleados y/o socios que se conectan remotamente a la red interna y que ha dado el paso importante de utilizar tecnología VPN para permitirles el acceso. Sin embargo, no ha utilizado autenticación multifactor como un segundo escudo protector.	Estudie utilizar la autenticación multifactor para la conexión de usuarios remotos a través de Internet a los recursos corporativos. Revise con regularidad la lista de acceso de los usuarios en el dispositivo VPN.
Subcategoría	**Mejores prácticas recomendadas**	
Segmentación	Utilice segmentos para impedir el acceso a extranet específicas por parte de fabricantes, socios o clientes. Cada segmento externo de la red debe permitir que sólo se encamine determinado tráfico hacia los hosts y puertos concretos de aplicaciones que proporcionan servicios a los clientes. Asegúrese de que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limite el acceso de los servicios de red suministrados, así como el acceso entre los segmentos de red.	
	Resultados	**Recomendaciones**
Segmentación	Su respuesta indica que los servicios ofrecidos en Internet no se alojan en la red de su empresa.	Si los servicios de Internet se exponen a otros servicios que van a albergarse en la red de la empresa, asegúrese de que los cortafuegos, la segmentación y los sistemas de detección de intrusiones protegen la

		infraestructura de la empresa de los ataques desde Internet.
Segmentación	Sus respuestas indican que la red presenta un sólo segmento.	Utilice segmentos para separar extranet específicas y el acceso de fabricantes, socios o clientes. Cada segmento externo de la red debe permitir que sólo el tráfico específico sea encaminado a hosts de aplicaciones específicos y a puertos utilizados para prestar servicios a los clientes. Asegúrese de que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limite el acceso a y de los servicios de red suministrados y entre los segmentos de red.
Subcategoría	**Mejores prácticas recomendadas**	
Sistema de detección de intrusiones (IDS)	Los sistemas de detección de intrusiones basados en host y en red deben implantarse para detectar y notificar cualquier ataque que se produzca contra los sistemas corporativos.	
	Resultados	**Recomendaciones**
Sistema de detección de intrusiones (IDS)	Sus respuestas indican que no utiliza ningún hardware ni software de detección de intrusiones.	Considere la implantación de sistemas de detección de intrusiones basados en red o en host.
Subcategoría	**Mejores prácticas recomendadas**	
Inalámbrico	Las mejores prácticas para la implantación inalámbrica incluyen la garantía de que la red no hace público su SSID, que se usa el cifrado WPA y que la red no se considera fundamentalmente como de no confianza.	
	Resultados	**Recomendaciones**
Inalámbrico	Sus respuestas indican que existe la opción de conexión inalámbrica a su red	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.
Inalámbrico	Su respuesta indica que no ha modificado el SSID predeterminado del punto de acceso.	Para evitar que se pueda abusar fácilmente del punto de acceso y de la red inalámbrica, debe cambiar inmediatamente el SSID a un valor que no se asocie fácilmente con su empresa.
Inalámbrico	Sus respuestas indican que no ha desactivado la difusión del SSID en el punto de acceso.	Considere la deshabilitación de la difusión del SSID para dificultar a un usuario ocasional los intentos de conexión a su red inalámbrica.
Inalámbrico	Sus respuestas indican que no utiliza el cifrado WEP en el entorno inalámbrico.	Si actualmente no está utilizando ningún cifrado, considere utilizar WPA para evitar que el tráfico de la red inalámbrica sea "detectado" y leído como texto sin formato.
Inalámbrico	Sus respuestas indican que utiliza el cifrado WPA en el entorno	En la actualidad, WPA es el estándar de cifrado más seguro pero aún se puede

	inalámbrico.	descodificar. Considere la utilización de un cifrado adicional (como VPN) para una mayor seguridad.
Inalámbrico	Sus respuestas indican que no utiliza la restricción por MAC en el entorno inalámbrico.	Considere el uso de autenticación WPA además de los filtros MAC, con el fin de evitar que ordenadores no autorizados se conecten a la red.
Inalámbrico	Sus respuestas indican que la red inalámbrica se considera de no confianza.	Considere migrar su red inalámbrica a un segmento de red de no confianza y exigir el uso de VPN o tecnologías similares para proteger mejor la integridad de los datos.

Tabla 8. Infraestructura

Tabla de Autenticación

Autenticación		
Subcategoría	**Mejores prácticas recomendadas**	
Usuarios administrativos	Ponga en práctica una directiva de contraseñas complejas para las cuentas administrativas con contraseñas que cumplan estas condiciones: + Alfanumérico + Mayúsculas y minúsculas + Contiene al menos un carácter especial + Contiene como mínimo 14 caracteres Para limitar más los riesgos de ataques a las contraseñas, ponga en práctica los controles siguientes: + Caducidad de contraseñas + Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos + Registro del sistema Además de las contraseñas complejas, puede recurrir a la autenticación multifactor. Utilice controles avanzados de la gestión de cuentas y del registro de acceso a cuentas (no permita que se compartan cuentas).	
	Resultados	**Recomendaciones**
Usuarios administrativos	Sus respuestas indican que los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo.	Considere eliminar el acceso administrativo de usuarios, para limitar la posibilidad de modificar la creación segura.
Usuarios administrativos	Sus respuestas indican que no se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas ni de los dispositivos del entorno.	Considere imponer cuentas separadas para las actividades administrativas o de gestión y asegúrese de que las credenciales administrativas se modifican con frecuencia.
Subcategoría	**Mejores prácticas recomendadas**	
Usuarios internos	Para las cuentas de usuario, implemente una directiva que requiera el uso de contraseñas complejas que cumplan los siguientes criterios:* Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres Para limitar aún más el riesgo de un ataque a contraseñas, implemente los siguientes	

	controles: * Caducidad de contraseña * Bloqueo de cuenta tras al menos 10 intentos de inicio de sesión erróneos * Registro del sistema Además de contraseñas complejas, considere la posibilidad de implementar una autenticación de varias fases. Implemente controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para el registro de acceso a cuentas.
Subcategoría	**Mejores prácticas recomendadas**
Usuarios de acceso remoto	Implemente controles de contraseña complejos para todos los usuarios de acceso remoto, si se ha concedido este acceso mediante el uso de tecnologías de acceso telefónico o VPN. Una contraseña se considera compleja si cumple los siguientes criterios:* Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres Implemente una fase adicional de autenticación para las cuentas a las que se ha concedido acceso remoto. Considere también la posibilidad de implementar controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para el registro de acceso a cuentas. En el caso del acceso remoto, resulta especialmente importante proteger el entorno mediante el uso de unas prácticas de gestión de cuentas segura, buenas prácticas de registro y capacidades de detección de incidentes. Para mitigar aún más los riesgos de ataques de fuerza bruta a contraseñas, considere la posibilidad de implementar los siguientes controles: * Caducidad de contraseña * Bloqueo de cuenta tras 7 a 10 intentos de inicio de sesión erróneos * Registro del sistema Los servicios de acceso remoto también deben tener en cuenta los sistemas que se utilizan para obtener acceso a redes o hosts. Considere también la posibilidad de implementar controles para hosts a los que se les permite acceder a la red de forma remota.
	Resultados / **Recomendaciones**
Usuarios de acceso remoto	Sus respuestas indican que los empleados no pueden conectarse a la red de forma remota. / Al no permitir el acceso remoto, reduce los riesgos globales. Sin embargo, si el acceso remoto se planea o se utiliza en el futuro, asegúrese de que lo hace conforme a la mejor práctica recomendada para minimizar así el riesgo asociado con esta forma de acceso.
Usuarios de acceso remoto	Sus respuestas indican que los contratistas pueden conectarse a la red de forma remota. / Además de permitir el acceso remoto a los empleados según las mejores prácticas recomendadas, considere limitar el acceso a los contratistas para que únicamente puedan acceder a los sistemas remotos necesarios. Por otro lado, plantéese utilizar un punto de entrada separado para los contratistas, con el fin de controlar y limitar su acceso con más facilidad.
Usuarios de acceso remoto	Sus respuestas indican que terceros usuarios no pueden conectarse a la red de forma remota. / Al no permitir el acceso remoto, reduce los riesgos globales. Sin embargo, si el acceso remoto se planea o se utiliza en el futuro, asegúrese de que lo hace conforme a la mejor práctica recomendada para minimizar

		así el riesgo asociado con esta forma de acceso.
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas	La utilización de contraseñas complejas es un elemento fundamental del índice de defensa en profundidad. Las contraseñas complejas deben tener de 8 a 14 caracteres e incluir caracteres alfanuméricos y especiales. Debe establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Además de las contraseñas complejas, la autenticación multifactor es muy importante, especialmente para las cuentas administrativas y de usuarios remotos. En todas las cuentas de usuario, se debe activar un proceso de bloqueo de cuenta tras 10 intentos de registro fallidos. Los controles para bloquear una cuenta pueden variar; algunos sencillamente se dedican a los ataques de fuerza bruta a las contraseñas y otros requieren que un administrador desbloquee la cuenta. Se considera una práctica aconsejable activar el bloqueo en las cuentas administrativas, al menos en lo que respecta al acceso a la red. De esta forma, la cuenta no se puede bloquear desde fuera de la consola, solamente desde la red. Es posible que esta solución no sea adecuada para todas las empresas, particularmente para aquellas con ubicaciones remotas. En tales casos, lo más adecuado es que un administrador desbloquee la cuenta, de este modo se evita que los ataques pasen desapercibidos durante largo tiempo si no se dispone de otros medios para detectar fallos de autenticación. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de entre 7 y 10 intentos de registro fallidos para las cuentas administrativas y de acceso remoto + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario estándar + Requerir la intervención de un administrador para desbloquear las cuentas de acceso remoto y de administrador, y para reactivar automáticamente las cuentas de usuarios estándar al cabo de 5 minutos.	
Directivas de contraseñas	Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se aplican a las cuentas normales. En sistemas Windows, debe establecer contraseñas de 14 caracteres alfanuméricos y especiales para las cuentas administrativas (y las cuentas de servicio).	
	Resultados	**Recomendaciones**
Directivas de contraseñas	Sus respuestas indican que no existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas.	Piense en implantar el uso de contraseñas complejas para todas las cuentas como en la sección de mejores prácticas recomendadas. Piense en implantar el uso de la caducidad de contraseñas como en la sección de mejores prácticas recomendadas.
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas-Cuenta de administrador		

Subcategoría	Mejores prácticas recomendadas	
Directivas de contraseñas-Cuenta de usuario		
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas-Cuenta de acceso remoto		
Subcategoría	**Mejores prácticas recomendadas**	
Cuentas inactivas	Continúe supervisando y gestionando cuentas inactivas.	
Cuentas inactivas	Establezca un proceso para incluir un procedimiento de notificación inmediata a todos los administradores del sistema para el personal que ya no está en la organización con el objeto de garantizar que sus cuentas se deshabiliten inmediatamente, especialmente sus cuentas de acceso remoto. Considere la posibilidad de implementar un proceso para revisar las cuentas actuales del personal que se transfiere a otro departamento dentro de la organización.	
Cuentas inactivas	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.	
Cuentas inactivas	Visite habitualmente los sitios de los fabricantes para obtener actualizaciones de las firmas de virus y descárguelas en un sitio aislado para probarlas en un entorno de laboratorio. Verifique que las actualizaciones no causen problemas con ningún sistema operativo ni aplicaciones antes de utilizarlas. Debe desactivar las funciones de actualización automática de las soluciones antivirus en todos los sistemas para evitar la utilización de archivos potencialmente peligrosos antes de su comprobación. Utilice una consola central para las aplicaciones antivirus, esta consola proporcionará información acerca de los sistemas obsoletos o con funciones de software desactivadas. Para los usuarios remotos que no se conectan regularmente a la red corporativa, puede usar la función de actualización automática.	
Cuentas inactivas	Las cuentas del personal que ya no está en la organización se deben deshabilitar a tiempo para garantizar que los usuarios eliminados u otros usuarios no puedan utilizar la cuenta para obtener acceso no autorizado. Si los administradores de sistemas no tienen información sobre los cambios del estado de un usuario debido a su transferencia, no cambiarán o quitarán los accesos al sistema o físicos. Esto puede dar lugar a un acceso no autorizado o excesivo por parte de los usuarios transferidos.	
	Resultados	**Recomendaciones**
Cuentas inactivas	Su respuesta indica que existen directivas para las actualizaciones de firmas de virus en el entorno.	Visite con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus Realice auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas. Trabaje conforme a las mejores prácticas recomendadas.

Cuentas inactivas	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.

Tabla 9. Autenticación

Tabla de Gestión y Control

Gestión y control		
Subcategoría	**Mejores prácticas recomendadas**	
Informes sobre incidentes y respuesta	Continúe aplicando y siguiendo procedimientos de creación de informes y respuesta ante incidentes formales	
Informes sobre incidentes y respuesta	Establezca procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad. Designe un equipo de respuesta de emergencia que incluya representantes de varias disciplinas, incluida tecnologías, recursos humanos y legales para responder a todos los incidentes y problemas de seguridad. Considere la posibilidad de implementar un programa completo de respuesta a incidentes que incluya equipos de respuesta a incidentes, gestión de contención, correlación y análisis de eventos, y procedimientos de repuesta a incidentes.	
Informes sobre incidentes y respuesta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.	
Informes sobre incidentes y respuesta	Los planes de recuperación ante desastres y de reanudación de negocio deben estar bien documentados y actualizados para asegurar la recuperación en un período de tiempo aceptable. Los planes (incluida la restauración a partir de copias de seguridad para aplicaciones) se deben probar periódicamente para validar el grado de corrección e integridad. Los planes de continuidad de negocio se deben centrar en todo el entorno: físico, tecnológico y personal.	
Informes sobre incidentes y respuesta	Es importante seguir un proceso de creación de informes de incidentes y repuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.	
Subcategoría	**Mejores prácticas recomendadas**	
Creación segura		
	Resultados	**Recomendaciones**
Creación segura	Sus respuestas indican que se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno.	Al principio, piense en utilizar cortafuegos particulares en cada equipo portátil. De manera predeterminada, bloquee todo acceso a la estación de trabajo desde el exterior.
Creación segura	Sus respuestas indican que los procesos de creación de los dispositivos de infraestructura están documentados.	Implante un proceso de creación documentado para los dispositivos de infraestructura y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación	Sus respuestas indican que no hay	Considere utilizar software de acceso remoto en

segura	software de acceso remoto del lado del cliente instalado en las estaciones de trabajo que se conectan remotamente a la red corporativa.	todas las estaciones individuales, si se necesita conectividad remota. Configure el software de cliente para seguir la directiva de servidores de acceso remoto.
Creación segura	Sus respuestas indican que los procesos de creación de los servidores están documentados.	Implante un proceso de creación documentado para los servidores y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación segura	Sus respuestas indican que no utiliza ningún software de cifrado de discos en el entorno.	Piense en utilizar software de cifrado de discos con el fin de no poner en peligro la confidencialidad de los datos en caso de robo del equipo.
Creación segura	Sus respuestas indican que los procesos de creación de las estaciones de trabajo y los portátiles están documentados.	Implante un proceso de creación documentado para las estaciones de trabajo y los portátiles, y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación segura	Sus respuestas indican que utiliza algún software de control/gestión remota en el entorno.	Considere la deshabilitación del software de gestión/control remoto para reducir el riesgo de intrusiones en los sistemas.
Creación segura	Sus respuestas indican que no utiliza ningún protector de pantalla protegido por contraseña en el entorno.	Considere exigir a todos los usuarios que tengan un protector de pantalla protegido por contraseña con un período de descanso breve.
Creación segura	Sus respuestas indican que no se utilizan módems en el entorno.	Continúe la deshabilitación del acceso por módem y marcación telefónica para reducir el riesgo de que se pueda acceder directamente a los equipos mediante marcación.
Subcategoría	**Mejores prácticas recomendadas**	
Seguridad física	Continúe implementando controles de acceso de seguridad física.	
Seguridad física	Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.	
Seguridad física	Todos los equipos informáticos se deben proteger contra robos. Los servidores y los equipos de red deben asegurarse en ubicaciones cerradas con acceso controlado.	
Seguridad física	El acceso físico se debe controlar estrictamente, evitando que las personas no autorizadas accedan a edificios, datos confidenciales y sistemas. Con este acceso, pueden alterar las configuraciones del sistema, introducir vulnerabilidades en la red o incluso destruir o robar equipos.	
	Resultados	**Recomendaciones**
Seguridad física	Sus respuestas indican que se han instaurado controles de seguridad física para proteger los activos de la empresa.	Continúe utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.
Seguridad física	Sus respuestas indican que no se ha instalado ningún sistema de alarma para detectar ni informar de intrusiones	Considere la instalación de un sistema de alarma con el fin de detectar e informar de intrusiones.

Seguridad física	La respuesta indica que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.
Seguridad física	Sus respuestas indican que los equipos de la red se hallan en una habitación cerrada con acceso restringido.	Continúe con la práctica de proteger equipo de red en una habitación cerrada y asegúrese de que únicamente acceden los que deben hacerlo por alguna actividad relacionada con la empresa.
Seguridad física	La respuesta indica que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.
Seguridad física	Sus respuestas indican que los equipos de la red se encuentran además en un armario cerrado.	Si el equipo de red se encuentra en un armario cerrado, la protección contra la manipulación no autorizada es adicional. Asegúrese de que el acceso a las llaves/combinaciones se limita a aquéllos que únicamente lo necesitan por alguna actividad relacionada con la empresa.
Seguridad física	La respuesta indica que todo o parte de lo siguiente está implementado. (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada)	Continúe implementando controles de acceso de seguridad física.
Seguridad física	Sus respuestas indican que los servidores se hallan en una habitación cerrada con acceso restringido.	Continúe la práctica de asegurar los servidores en una habitación cerrada y asegúrese de que únicamente acceden los que deben hacerlo por alguna actividad relacionada con la empresa.
Seguridad física	La respuesta indica que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.
Seguridad física	Sus respuestas indican que los servidores no se encuentran en un	Si los servidores se encuentran en un armario cerrado, la protección contra la manipulación no

	armario cerrado.	autorizada es adicional. Si es posible, considere migrar los servidores a recintos que se puedan cerrar con llave.
Seguridad física	Sus respuestas indican que las estaciones de trabajo no están protegidas con cables de seguridad.	Para evitar robos, considere asegurar las estaciones de trabajo con cables de seguridad.
Seguridad física	Sus respuestas indican que los ordenadores portátiles no están protegidos con cables de seguridad.	Para evitar robos, considere asegurar los portátiles mediante cables de seguridad.
Seguridad física	Sus respuestas indican que los materiales impresos confidenciales no se almacenan en armarios con llave.	Los documentos confidenciales deberían guardarse en armarios cerrados para que no resulten robados ni se revele información confidencial.

Tabla 10. Gestión y Control

5.3.8. Aplicaciones

Una comprensión total de la seguridad de las aplicaciones requiere un conocimiento profundo de la arquitectura de las aplicaciones subyacentes básicas, así como de un conocimiento sólido de la base de la aplicación del usuario. Sólo entonces podrá comenzar a identificar las posibles amenazas.

Teniendo en cuenta el ámbito limitado de esta autoevaluación, no es posible un análisis completo de la arquitectura de las aplicaciones ni una comprensión completa de la base del usuario. El objetivo de esta evaluación consiste en ayudarle a revisar las aplicaciones de su empresa y valorarlas desde el punto de vista de la seguridad y disponibilidad. Examina las tecnologías utilizadas en el entorno para contribuir a mejorar la defensa en profundidad. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos para la infraestructura centrándose en las siguientes áreas de seguridad:

- Utilización y uso—mecanismos para mejorar la disponibilidad
- Diseño de aplicaciones —autenticación, control de acceso, gestión de actualizaciones, validación de datos de entrada, registros y auditorías
- Almacenamiento y comunicaciones de datos—cifrado, transferencia de datos, acceso restrictivo

Tabla de Implementación y Uso

Implementación y uso		
Subcategoría	**Mejores prácticas recomendadas**	
Equilibrio de carga		
	Resultados	**Recomendaciones**
Equilibrio de carga	Sus respuestas indican que no se utilizan equilibradores de carga en el entorno.	Piense en utilizar equilibradores de carga de hardware en el primer nivel de los servidores Web para obtener una mayor disponibilidad. El equilibrador de carga muestra una sola dirección IP (virtual) al exterior que se asigna a todas las direcciones de cada servidor Web en el clúster.
Subcategoría	**Mejores prácticas recomendadas**	
Clústeres		
	Resultados	**Recomendaciones**
Clústeres	Sus respuestas indican que no se utiliza la agrupación en clústeres en el entorno.	Para asegurar una disponibilidad alta de las bases de datos críticas y de los archivos compartidos, piense en utilizar mecanismos de clúster.
Subcategoría	**Mejores prácticas recomendadas**	
Aplicación y recuperación de datos		
	Resultados	**Recomendaciones**
Aplicación y recuperación de datos	Sus respuestas indican que su empresa tiene una línea de aplicaciones empresariales	Todas las aplicaciones de líneas comerciales deberían evaluarse periódicamente para su seguridad, someterse a procesos regulares de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.
Aplicación y recuperación de datos	Su respuesta indica que no se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.	Realice copias de seguridad regularmente. Pruebe regularmente el mecanismo de copias de seguridad y recuperación que restaura la aplicación a un estado normal de operación.
Subcategoría	**Mejores prácticas recomendadas**	
Fabricante de software independiente (ISV)	Los fabricantes de software independiente (ISV) deben ofrecer revisiones y actualizaciones periódicas, en las que se explique su finalidad y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El ISV debe identificar claramente cuáles son las actualizaciones más importantes para que se apliquen rápidamente. Asimismo, debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más reciente. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto.	
	Resultados	**Recomendaciones**
Fabricante de software independiente (ISV)	Sus respuestas indican que otros fabricantes no han desarrollado ninguna de las aplicaciones principales del	Continúe desarrollando aplicaciones clave propias, pero si posteriormente decide obtenerlas de un tercero, asegúrese de que podrá seguir disponiendo de servicio técnico y actualizaciones

	entorno.	periódicas para los software clave de su empresa, o que el fabricante independiente de los mismos puede ofrecerle el código de origen en caso de que ya no pueda prestar dicho servicio para la aplicación.
Subcategoría	**Mejores prácticas recomendadas**	
Desarrollado internamente	El equipo de desarrollo interno debe proporcionar las actualizaciones y revisiones e indicar cuál es la finalidad de la actualización y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El equipo de desarrollo interno debe identificar claramente cuáles son las actualizaciones más importantes para que la empresa pueda instalarlas rápidamente. El equipo de desarrollo debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más actualizada. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto. Considere la posibilidad de contratar servicios independientes para revisar la arquitectura y utilización de la aplicación y para identificar los problemas de seguridad que pudieran existir.	
	Resultados	**Recomendaciones**
Desarrollado internamente	Sus respuestas indican que su empresa no utiliza macros personalizadas en las aplicaciones ofimáticas.	No continúe utilizando macros de Office personalizadas, ya que es necesario que las configuraciones de seguridad de Office se reclasifiquen a un nivel inferior, por lo que sus aplicaciones ofimáticas quedan expuestas a documentos peligrosos.
Subcategoría	**Mejores prácticas recomendadas**	
Vulnerabilidades	Debe identificar y corregir todas las vulnerabilidades de seguridad conocidas. Visite los sitios de los fabricantes y otros proveedores de soluciones de seguridad para buscar información sobre nuevas vulnerabilidades, así como las actualizaciones disponibles. Si no existen actualizaciones disponibles para vulnerabilidades de seguridad conocidas, intente averiguar cuándo podrá disponer de una y desarrolle un plan de seguridad provisional. Puede contratar servicios independientes para revisar regularmente el diseño de seguridad de la aplicación. Una evaluación realizada por terceros podría descubrir otros problemas que exijan mecanismos de seguridad adicionales.	
	Resultados	**Recomendaciones**
Vulnerabilidades	Su respuesta indica que actualmente no se conocen vulnerabilidades para la seguridad en ninguna aplicación de su entorno.	Visite los sitios de los fabricantes y otros proveedores de soluciones de seguridad para detectar vulnerabilidades de la aplicación. Piense en una evaluación independiente para que un tercero pueda valorar el diseño de la seguridad de la aplicación e identificar otros problemas que necesiten más mecanismos de seguridad.

Tabla 11. Implementación y Uso

Tabla de Diseño de Aplicaciones

Diseño de aplicaciones		
Subcategoría	**Mejores prácticas recomendadas**	
Autenticación	La aplicación debe utilizar un mecanismo de autenticación cuya eficacia sea proporcional a las necesidades de seguridad de los datos o de su funcionalidad. Las aplicaciones que dependen de contraseñas deben requerir contraseñas complejas que incluyan diversos caracteres (alfabéticos, numéricos, y símbolos), una longitud mínima, un historial, un límite de duración, una pre-caducidad y una comprobación en el diccionario. La aplicación debe archivar los intentos de registro fallidos, pero no la contraseña. Cada componente que concede acceso a datos o a funciones debe requerir una autenticación correcta. Debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las de las cuentas normales. Además de usar contraseñas sólidas con directivas de contraseñas, considere la autenticación multifactor para una mayor seguridad.	
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas	La utilización de contraseñas sólidas es un elemento fundamental del índice de la defensa en profundidad. Estas contraseñas deben tener entre 8 y 14 caracteres e incluir caracteres alfanuméricos y especiales. Debe establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se emplean para cuentas normales: si las cuentas normales requieren contraseñas con 8 caracteres, las cuentas administrativas deben requerir contraseñas de 14 caracteres. Active una práctica de bloqueo de la cuenta tras 10 intentos fallidos en todas las cuentas de usuario. Los controles para bloquear una cuenta pueden variar, algunos simplemente consisten en bloquear ataques de fuerza bruta a contraseñas y otros requieren que un administrador desbloquee la cuenta. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario + Requerir la intervención de un administrador para desbloquear las cuentas de aplicaciones importantes y reactivar automáticamente las cuentas de usuarios normales al cabo de 5 minutos + 30 minutos para almacenar en caché los fallos de cuentas de usuarios normales	
	Resultados	**Recomendaciones**
Directivas de contraseñas	Su respuesta indica que no se usan controles de contraseñas en las aplicaciones principales.	Es importante poner en práctica una directiva de controles de contraseña. Todas las aplicaciones externas e internas importantes con datos confidenciales deben tener directivas de contraseñas.

		Piense en poner en práctica una directiva que requiera contraseñas complejas, períodos de caducidad de contraseñas y umbrales para bloquear las cuentas.
Subcategoría	**Mejores prácticas recomendadas**	
Autorización y control de acceso	Las aplicaciones deben utilizar un mecanismo de autorización que permita sólo a los usuarios o clientes adecuados el acceso a datos y funciones confidenciales. Debe mantener controles de acceso basados en roles, tanto para la base de datos como para la interfaz de la aplicación. De esta forma, se protege la base de datos incluso si la aplicación cliente resulta atacada. Para comprobar una autorización, deberá haberse realizado antes una autenticación con éxito. Se deben archivar todos los intentos de acceso sin autorización adecuada. Compruebe regularmente las aplicaciones principales que procesan datos confidenciales y las interfaces disponibles a los usuarios de Internet. Incluya pruebas de "caja negra" e "informadas" de la aplicación. Descubra si los usuarios pueden acceder a los datos mediante otras cuentas.	
	Resultados	**Recomendaciones**
Autorización y control de acceso	Su respuesta indica que las aplicaciones principales limitan el acceso a datos y funciones confidenciales según los privilegios de la cuenta.	Piense en probar exclusivamente las aplicaciones principales que procesen datos confidenciales y las interfaces disponibles para los usuarios por Internet. Incluya pruebas tipo "caja negra" e "informadas" de la aplicación y compruebe la asignación de mayores privilegios.
Subcategoría	**Mejores prácticas recomendadas**	
Registro	Debe activar archivos de registro en todas las aplicaciones del entorno. Los datos de archivos de registro son importantes para los análisis de incidentes, tendencias y auditorías. La aplicación debe registrar los intentos de autenticación que tienen éxito y los fallidos, además de los cambios de datos de la aplicación, incluidas las cuentas de usuarios, los errores graves de la aplicación y los accesos correctos y fallidos a los recursos. Cuando escriba datos en los archivos de registro, la aplicación deberá evitar los de carácter confidencial.	
	Resultados	**Recomendaciones**
Registro	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise esta opción abierta con su personal de TI o con un socio de seguridad. Introduzca la respuesta más adecuada a esta pregunta en MSAT para obtener más información.
Subcategoría	**Mejores prácticas recomendadas**	
Validación de datos de entrada	La aplicación puede permitir la entrada de datos en distintos puntos a partir de fuentes externas, como, por ejemplo, usuarios, aplicaciones de cliente o bien alimentación de datos. Será necesario comprobar que los datos de entrada tengan una sintaxis y semántica correctas. Por otro lado, se comprobará si tales datos cumplen las restricciones de los componentes subyacentes o dependientes,	

	particularmente la longitud de cadenas y los juegos de caracteres. El servidor deberá validar los campos suministrados por el usuario.	
	Resultados	**Recomendaciones**
Validación de datos de entrada	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise esta opción abierta con su personal de TI o con un socio de seguridad. Introduzca la respuesta más adecuada a esta pregunta en MSAT para obtener más información.
Subcategoría	**Mejores prácticas recomendadas**	
Metodologías de desarrollo de seguridad de software	Continúe utilizando las metodologías de desarrollo de seguridad de software.	
Metodologías de desarrollo de seguridad de software	Establezca el uso de metodologías de desarrollo de seguridad de software para aumentar la seguridad de las aplicaciones.	
Metodologías de desarrollo de seguridad de software	Si se utilizan consultores o proveedores en alguna fase del ciclo de desarrollo, asegúrese de que tienen formación en la metodología de desarrollo de seguridad de software que la organización utilice o recomiende.	
Metodologías de desarrollo de seguridad de software	Todo el personal de desarrollo de su organización debe recibir formación sobre la metodología de desarrollo de seguridad para software que la organización ha elegido. Esto incluye administradores de desarrollo, desarrolladores, evaluadores y personal de control de calidad.	
Metodologías de desarrollo de seguridad de software	Con el panorama de evolución de amenazas de seguridad, es importante actualizar la formación sobre metodologías de desarrollo de seguridad de software y modelos de amenazas anualmente. Se le solicitará al personal de desarrollo que siga la formación sobre desarrollo de seguridad cada año.	
Metodologías de desarrollo de seguridad de software	El uso de herramientas de prueba de software de seguridad mejora la capacidad del equipo para escribir código seguro con más eficacia. El resultado del uso de las herramientas de prueba se debe incorporar a la formación anual necesaria.	
	Resultados	**Recomendaciones**
Metodologías de desarrollo de seguridad de software	La respuesta indica que su organización utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.	Amplíe el uso de las herramientas de prueba de software de seguridad como parte instrumental de todos los planes de desarrollo de seguridad.
Metodologías de desarrollo de seguridad de software	La respuesta indica que su organización no proporciona formación sobre metodologías de seguridad para software para su personal de desarrollo.	Establezca un programa de formación de metodologías de desarrollo de seguridad de software con el objeto de mejorar la capacidad del personal para desarrollar código seguro.

Tabla 12. Diseño de Aplicaciones

Tabla de Almacenamiento y comunicaciones de datos

Almacenamiento y comunicaciones de datos		
Subcategoría	**Mejores prácticas recomendadas**	
Cifrado	Los datos confidenciales deben cifrarse o codificarse mediante hash en la base de datos y en el sistema de archivos. La aplicación debe diferenciar entre los datos que podrían estar expuestos a la divulgación (es necesario cifrarlos), los datos que podrían llegar a manipularse (es necesario un valor de claves hash) y los datos que se pueden transformar (hash) sin ninguna pérdida de funcionalidad, como las contraseñas. Las claves para descifrar se guardarán en un lugar distinto a la información cifrada. Los datos confidenciales se deben cifrar antes de transmitirlos a otros componentes. Verifique que los componentes intermedios que controlan los datos en un formato de texto sin formato antes o después de la transmisión no representan una amenaza excesiva. La aplicación debe sacar partido de las funciones de autenticación disponibles con el mecanismo de transmisión segura. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Utilice claves de 128 bits (1024 bits para RSA) como mínimo.	
	Resultados	**Recomendaciones**
Cifrado	Sus respuestas indican que sus aplicaciones no cifran los datos cuando están almacenados o se están transmitiendo.	Para aplicaciones que procesan datos confidenciales, opte por el cifrado con un algoritmo estándar del sector para la transmisión y el almacenamiento de datos.
Subcategoría	**Mejores prácticas recomendadas**	
Cifrado - Algoritmo	La aplicación debe utilizar algoritmos de cifrado estándares del sector, con claves de tamaños adecuados y modelos de cifrado apropiados. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Se debe utilizar un tamaño de clave mínimo de 128 bits (para RSA, 1024 bits).	

Tabla 13. Almacenamiento y comunicaciones de datos

5.3.9. Operaciones

Esta área de análisis examina las prácticas, procedimientos y pautas operativas que sigue la empresa para ayudar a mejorar la defensa en profundidad. Esta evaluación examina directivas y procedimientos que regulan las creaciones del sistema, la documentación de la red y el uso de tecnología en el entorno. También incluye las actividades de apoyo necesarias para gestionar la información y los procedimientos que utilizan los administradores y el equipo de operaciones en el entorno. Al establecer prácticas, procedimientos y pautas operativas que se entienden y se siguen, una empresa tiene la posibilidad de mejorar su defensa en profundidad. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a

mitigar los riesgos para la infraestructura centrándose en las siguientes áreas de seguridad de las operaciones:

- Entorno—creación del sistema, documentación de la red, flujo de datos de aplicación, arquitectura de las aplicaciones
- Directiva de seguridad—protocolos y servicios, uso aceptable, gestión de cuentas de usuarios
- Actualizaciones y gestión de actualizaciones—gestión de actualizaciones, firmas de virus
- Copias de seguridad y recuperación—copias de seguridad, almacenamiento, pruebas

Tabla de Entorno

Entorno		
Subcategoría	**Mejores prácticas recomendadas**	
Host de gestión	Cuando se utilizan paquetes de gestión, las consolas administrativas se deberán reforzar y proteger físicamente.Refuerce las estaciones de trabajo de gestión utilizadas para gestionar los servidores y dispositivos de red. Utilice conexiones SSH o VPN para proteger los protocolos de gestión de texto sin cifrar. Las estaciones de trabajo de gestión se deben dedicar a administradores de red y host específicos. Pruebe todos los sistemas de gestión que utilizan SNMP para asegurarse de que tienen la revisión de la última versión y no utilizan cadenas de comunidad predeterminadas. Los sistemas compartidos no almacenan datos específicos de gestión. No se utilizan estaciones de trabajo compartidas para gestionar dispositivos de red o hosts.	
	Resultados	**Recomendaciones**
Host de gestión	Su respuesta indica que no existen equipos de gestión dedicados a la administración de sistemas y dispositivos del entorno.	Piense en utilizar estaciones de trabajo de gestión distintas para administrar los servidores y dispositivos de red por un protocolo seguro. Utilice SSH o VPN para asegurar los protocolos de gestión de texto sin formato. Debe reforzar las estaciones de trabajo de administración y poner en práctica controles de contraseñas fuertes basados en las capacidades del sistema host y las aplicaciones de gestión.
Subcategoría	**Mejores prácticas recomendadas**	
Host de gestión-Servidores		
Subcategoría	**Mejores prácticas recomendadas**	
Host de gestión - Dispositivos de red		

Tabla 14. Entorno

Tabla de Directiva de Seguridad

Directiva de seguridad		
Subcategoría	**Mejores prácticas recomendadas**	
Clasificación de datos	Continúe implementando clasificaciones de datos con las directrices de protección correspondientes.	
Clasificación de datos	Defina un esquema de clasificación de datos corporativos y proporcione a todo el personal una guía y un proceso de formación adecuados acerca de la clasificación de datos. Defina requisitos de manejo y protección útiles correspondientes a los niveles de clasificación de datos.	
Clasificación de datos	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.	
Clasificación de datos	Es importante tener un esquema de clasificación de datos con las directrices de protección de datos correspondientes. Una “clasificación” y separación de la información insuficientes pueden permitir el acceso al personal, socios comerciales o público a información confidencial o a información que no necesiten saber. Esto puede suponer una pérdida de la imagen de marca o una situación comprometida de la empresa debido a la divulgación no autorizada de información confidencial. Es posible que los escasos recursos utilizados para asegurar la información también se asignen erróneamente sin la clasificación adecuada de la información. Si el personal no sabe qué información de la empresa es confidencial y cómo se protegen estos datos, existe una alta probabilidad de que esta información quede expuesta a personas no autorizadas.	
	Resultados	**Recomendaciones**
Clasificación de datos	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.
Subcategoría	**Mejores prácticas recomendadas**	
Eliminación de datos	Continúe implementando procesos para la eliminación de datos.	
Eliminación de datos	Defina e implemente procedimientos para la gestión y la eliminación de información en formato impreso y electrónico, como la que contienen disquetes y discos duros.	
Eliminación de datos	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.	
Eliminación de datos	También deben existir procedimientos formales de forma que todos los usuarios conozcan los procedimientos adecuados para eliminar información electrónica y en formato impreso. La confidencialidad de la información se puede ver en peligro si no se proporcionan instrucciones y procesos para destruir la información de forma segura.	
	Resultados	**Recomendaciones**
Eliminación de datos	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.
Subcategoría	**Mejores prácticas recomendadas**	
Protocolos y servicios	Documente las normas y las prácticas permitidas con respecto a los protocolos y servicios admitidos por la empresa. Se deben verificar las listas de control de acceso para garantizar que los servicios permitidos tienen necesidades empresariales acordes con el nivel de acceso de que disponen. Utilice direcciones IP y rangos de	

	direcciones IP específicos donde sea posible. Limite los servicios de los servidores a los que necesita la empresa. Estas pautas detallarán también las cuestiones específicas para la versión de protocolo y la fiabilidad mínima del cifrado. Implante el uso de protocolos establecidos con dispositivos del perímetro (como encaminadores, pasarelas, cortafuegos, etc.), la autenticación sólida y las comunicaciones cifradas.	
	Resultados	**Recomendaciones**
Protocolos y servicios	Su respuesta indica que no existen pautas que traten los servicios ni protocolos permitidos.	Colabore con el equipo de seguridad y comercial para establecer las pautas de los protocolos y servicios permitidos en el entorno corporativo y documente estas pautas. A continuación, audite los dispositivos necesarios (cortafuegos, dispositivos VPN, encaminadores, etc.) para asegurarse de que están configurados de forma acorde a las pautas documentadas.
Subcategoría	**Mejores prácticas recomendadas**	
Uso aceptable	Existe una directiva corporativa del uso aceptable que gestiona el buen uso de las redes corporativas, las aplicaciones, los datos y los sistemas. La directiva también debe comprender los medios digitales, los medios impresos y otras propiedades intelectuales.	
Subcategoría	**Mejores prácticas recomendadas**	
Gestión de cuentas de usuarios	Debe crear una cuenta de usuario individual para todo aquel que necesite acceso a los recursos de TI. Los usuarios no deben compartir cuentas. De forma predeterminada, las cuentas se crearán con los privilegios mínimos necesarios. Los administradores de las redes y los servidores deben tener una cuenta con privilegios (administrativa) y otra sin privilegios. Se impondrá la calidad de las contraseñas, se revisarán periódicamente y se registrarán todos los cambios en las cuentas. A medida que cambie el rol de un individuo, revise y modifique los privilegios de su cuenta, según sea necesario. Cuando se prescinda de algún miembro del personal, se deberá desactivar o eliminar su cuenta.	
Subcategoría	**Mejores prácticas recomendadas**	
Regulación	Las auditorías efectuadas por terceros deben realizarse periódicamente para garantizar que se cumple con todas las regulaciones legales y civiles vigentes (por ejemplo, HIPAA para la salud o Sarbanes-Oxley para las empresas conforme a la norma SEC).	
	Resultados	**Recomendaciones**
Regulación	Sus respuestas indican que su empresa no dispone de directivas para controlar el entorno informático.	Las directivas son reglas y prácticas que especifican cómo se puede utilizar de forma adecuada un entorno informático. Si no existen directivas, no existe mecanismo alguno para definir ni hacer cumplir los controles dentro del entorno. Planifique inmediatamente el desarrollo de las directivas necesarias de acuerdo con los estándares de aplicación y gestión de la compañía.
Subcategoría	**Mejores prácticas recomendadas**	
Directiva de seguridad	Las directivas de seguridad deben establecerse según la información suministrada desde los cargos de gestión, de TI y recursos humanos; deben ponerlas en funcionamiento los ejecutivos; y se deben actualizar para reflejar las mejores prácticas recomendadas como, por ejemplo, CoBIT.	

Tabla 15. Directiva de Seguridad

Tabla de Gestión de actualizaciones y revisiones

.Gestión de actualizaciones y revisiones		
Subcategoría	**Mejores prácticas recomendadas**	
Documentación de la red	Los diagramas actuales y precisos de las relaciones físicas y lógicas de las redes internas y externas tendrán que estar disponibles en todo momento. Actualice estos diagramas conforme se produzcan cambios en el entorno. Limite el acceso a los diagramas a sólo el equipo de TI.	
	Resultados	**Recomendaciones**
Documentación de la red	Su respuesta indica que no existen diagramas lógicos de red en su entorno.	Trabaje con el grupo de ingenieros de red para que desarrollen en primer lugar los diagramas de la red externa. A continuación, dedíquese a los diagramas de la red interna. Limite el acceso a estos diagramas a un grupo del personal, principalmente a los equipos de TI y de seguridad.
Subcategoría	**Mejores prácticas recomendadas**	
Flujo de datos de la aplicación	Los diagramas de la arquitectura de las aplicaciones deben mostrar los principales componentes y los flujos de datos fundamentales del entorno, además de los sistemas por los que pasa el tráfico de información y cómo se gestionan estos datos. Actualice los diagramas conforme surjan cambios en la aplicación o el entorno donde se alberga la aplicación.	
	Resultados	**Recomendaciones**
Flujo de datos de la aplicación	Su respuesta indica que no existen diagramas de la arquitectura ni del flujo de datos de las aplicaciones principales.	Trabaje con los propietarios de las empresas y dé prioridad a las aplicaciones externas sobre las internas. A continuación, sopese la importancia y confidencialidad de los datos que controla A partir de estas prioridades, colabore con el equipo de arquitectura de la aplicación y los propietarios de las empresas respectivas para completar los diagramas de arquitectura y de flujo de datos de las aplicaciones externas. Realice el mismo proceso para las aplicaciones internas. Evalúe la creación de una directiva para actualizar estos diagramas cuando el entorno se cambie.
Subcategoría	**Mejores prácticas recomendadas**	
Gestión de actualizaciones	Se aplicarán actualizaciones de seguridad y cambios de configuración en intervalos periódicos indicados por las directivas de seguridad corporativa y en el momento en que estén disponibles. Estas actualizaciones y revisiones se comprobarán exhaustivamente en un entorno de laboratorio antes de su instalación definitiva, con independencia de si se desarrollan internamente o se obtienen de un tercero. Por otra parte, una vez instaladas, se probarán cada uno de los sistemas para detectar conflictos exclusivos que podrían demandar desinstalar la actualización. Debe clasificar los sistemas para permitir una programación basada en agrupaciones: los sistemas más importantes y los que tienen más tráfico tendrán preferencia a la hora de recibir actualizaciones.	
	Resultados	**Recomendaciones**
Gestión de actualizaciones	Su respuesta indica que no existen directivas que regulen la gestión de actualizaciones ni revisiones	Desarrolle una directiva para la actualización de los sistemas operativos y todas las aplicaciones utilizando las pautas de prácticas recomendadas. Actualice en primer lugar los sistemas externos y de

	de los sistemas operativos y de las aplicaciones.	Internet, a continuación, los sistemas internos críticos y, por último, todos los sistemas no críticos. Desarrolle una directiva para notificar a los usuarios remotos cuándo aparecen actualizaciones, para que también las apliquen a sus sistemas.
Subcategoría	**Mejores prácticas recomendadas**	
Gestión de cambios y configuración	Cualquier cambio que se produzca en el entorno debe probarse primero para verificar que es seguro y compatible antes de ponerlo en producción. También se debe guardar una documentación completa acerca de la configuración de todos los sistemas de producción.	
	Resultados	**Recomendaciones**
Gestión de cambios y configuración	Sus respuestas indican que su empresa no dispone de ningún proceso de gestión de cambios ni configuraciones.	Considere la puesta en práctica de un proceso formal de gestión para las configuraciones y los cambios para probar y documentar todas las actualizaciones antes de su puesta en práctica.

Tabla 16. Gestión de actualizaciones y revisiones

Tabla de Copias de seguridad y recuperación

Copias de seguridad y recuperación		
Subcategoría	**Mejores prácticas recomendadas**	
Archivos de registro	Los archivos de registro se configuran para que graben las actividades planificadas sin sobrescribir entradas. Debe establecer un proceso automático de rotación de los archivos de registro cada día, así como la descarga de los archivos a un servidor seguro en la red de gestión. Limite el acceso a los archivos de registro y las configuraciones para evitar que sean modificados o eliminados. Los archivos de registro se deben revisar periódicamente para detectar actividades sospechosas o anómalas. La revisión debe extenderse al funcionamiento, mantenimiento y a la seguridad de los sistemas. Para sacar más partido de esta revisión, debe utilizar un software de correlación de eventos y de análisis de tendencias.	
	Resultados	**Recomendaciones**
Archivos de registro	Sus respuestas indican que actualmente no existe ningún registro activado en el entorno.	Al principio, active los archivos de registro en los servidores y los dispositivos en la DMZ, y también en los servidores de red centrales. Mantenga idénticas las configuraciones de los archivos en los varios sistemas y proteja el acceso a los archivos de registro para que no sean modificados ni eliminados. Piense en utilizar Microsoft Operations Manager (MOM) para enviar alertas cuando se produzcan entradas críticas de archivos de registro.
Subcategoría	**Mejores prácticas recomendadas**	
Planificación de	Continúe manteniendo y probando planes de recuperación ante desastres y de	

recuperación ante desastres y reanudación de negocio	reanudación de negocio.	
Planificación de recuperación ante desastres y reanudación de negocio	Es necesario desarrollar, documentar, implementar y someter los planes de recuperación ante desastres a revisiones, pruebas y actualizaciones periódicas. Desarrolle planes de continuidad de negocio que incluyan personal, ubicaciones, así como sistemas y otras cuestiones de tecnología.	
Planificación de recuperación ante desastres y reanudación de negocio	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.	
Planificación de recuperación ante desastres y reanudación de negocio	Los planes de recuperación ante desastres y de reanudación de negocio deben estar bien documentados y actualizados para asegurar la recuperación en un período de tiempo aceptable. Los planes (incluida la restauración a partir de copias de seguridad para aplicaciones) se deben probar periódicamente para validar el grado de corrección e integridad. Los planes de continuidad de negocio se deben centrar en todo el entorno: físico, tecnológico y personal.	
	Resultados	**Recomendaciones**
Planificación de recuperación ante desastres y reanudación de negocio	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.
Subcategoría	**Mejores prácticas recomendadas**	
Copias de seguridad	Debe realizar copias de seguridad completas con regularidad. Si le resulta posible, realice copias de seguridad parciales entre las completas. La estrategia de copias de seguridad debe abordar el problema más grave que podría presentarse: la restauración de la totalidad de sistemas y aplicaciones. Para aplicaciones críticas, el proceso de restauración debe realizarse en un tiempo mínimo y con garantías de un funcionamiento pleno.	
	Resultados	**Recomendaciones**
Copias de seguridad	Su respuesta indica que no se hacen copias de seguridad periódicas de los recursos críticos.	Identifique los recursos críticos de acuerdo con las necesidades empresariales y ponga en práctica un mecanismo para realizar copias de seguridad de estos recursos según las mejores prácticas recomendadas.
Subcategoría	**Mejores prácticas recomendadas**	
Dispositivos de copia de seguridad	Deben existir directivas detalladas para administrar el almacenamiento y la gestión de los dispositivos de copias de seguridad. Estas directivas deben abordar temas como:+ Almacenamiento en las instalaciones o fuera de ellas + Rotación de los dispositivos + Controles de seguridad + Controles de acceso para empleados Los dispositivos extraíbles de copias de seguridad deben almacenarse en armarios cerrados, a prueba de fuego, a los que sólo tengan acceso los empleados autorizados. El almacenamiento fuera de las instalaciones propicia la recuperación adicional de	

	datos en caso de producirse algún desastre.
Subcategoría	**Mejores prácticas recomendadas**
Copias de seguridad y restauración	Debe probar regularmente los procedimientos de copia de seguridad y de restauración para identificar dispositivos defectuosos y para mejorar las posibilidades de éxito de una restauración en caso de un apagón. Los procedimientos detallados para la restauración de los distintos sistemas, incluidas las aplicaciones, deben estar bien documentados. Revise los documentos de copias de seguridad y restauración para asegurarse de que cubren los aspectos relativos a los sistemas necesarios para la continuación de la actividad empresarial.

Tabla 17. Copias de seguridad y recuperación

5.3.10. Personal

Los esfuerzos de seguridad en una empresa a menudo pasan por alto los aspectos que son críticos para la ayuda del mantenimiento de la seguridad general en la empresa. Esta sección de la evaluación revisa aquellos procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la formación y la divulgación de materias de seguridad para los empleados. El área de análisis de personal también se centra en la seguridad, ya que relaciona las tareas diarias operativas y las definiciones de los roles. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos del personal centrándose en las siguientes áreas de la seguridad del personal:

- Requisitos y evaluaciones—planificación, evaluaciones de terceros
- Directiva y procedimientos—directiva de RR.HH., relaciones con terceros
- Formación y conocimiento—divulgación de las medidas de seguridad

Tabla de Requisitos y evaluaciones

Requisitos y evaluaciones		
Subcategoría	**Mejores prácticas recomendadas**	
Requisitos de seguridad	La empresa identifica a los individuos con experiencia en el tema de la seguridad para incluirlos en todas las reuniones y decisiones relacionadas. Además, señala qué debe protegerse, teniendo en cuenta el valor del recurso y el nivel de seguridad que se requiere. El análisis incluye todas las amenazas posibles. La estrategia que resulta equilibra los costes y los beneficios de las protecciones, y puede incluir como opciones el traslado o la aceptación de los riesgos. Los requisitos de seguridad, definidos por representantes comerciales y técnicos, se documentan y publican para que el conjunto del personal los pueda consultar y contrastar para diseños futuros. Las diferencias entre los tipos de aplicaciones y de datos pueden dar como resultado la existencia de requisitos diferentes.	
	Resultados	**Recomendaciones**
Requisitos de seguridad	Sus respuestas indican que su empresa no tiene ningún modelo para la asignación de niveles de gravedad a cada componente del entorno informático.	La asignación de niveles de importancia a cada componente de la infraestructura informática permite que la mayoría de los recursos se apliquen a aquéllos equipos establecidos como los más críticos, por lo que los sistemas que son menos críticos reciban menos recursos. Como consecuencia, se aplican con mayor eficacia los escasos recursos de seguridad en aquellos sistemas que los necesitan más.
Subcategoría	**Mejores prácticas recomendadas**	
Evaluaciones de seguridad	Las evaluaciones por parte de terceros aportan una perspectiva objetiva muy valiosa para las medidas de seguridad de una empresa. Estas evaluaciones también podrían resultar beneficiosas para cumplir las estipulaciones normativas y los requisitos de los clientes, socios y fabricantes. Las evaluaciones deben incluir la infraestructura, las aplicaciones, las directivas y los procedimientos de auditoría. Estas evaluaciones no deben centrarse exclusivamente en la identificación de vulnerabilidades, sino también en señalar configuraciones que no sean seguras o privilegios de acceso innecesarios. Se deben revisar las directivas y los procedimientos de seguridad para descubrir si tienen lagunas.	
	Resultados	**Recomendaciones**
Evaluaciones de seguridad	Su respuesta indica que no encarga a empresas independientes la evaluación de los medios de seguridad.	Empiece con autoevaluaciones de la infraestructura crítica de red y de las aplicaciones. Estudie desarrollar un plan que solicite evaluaciones regulares realizadas por terceros para la infraestructura crítica de red y de las aplicaciones. Incluya los resultados de las evaluaciones en sus proyectos de mejora.
Evaluaciones de seguridad	Sus respuestas indican que las evaluaciones de la seguridad de su empresa no las realiza personal interno.	Piense en el personal interno para la realización de auditorías de seguridad frecuentes, pero debe aumentar estas auditorías con los datos de un tercero de confianza.

Tabla 18. Requisitos y evaluaciones

Tabla de Directiva y procedimientos

Directiva y procedimientos		
Subcategoría	**Mejores prácticas recomendadas**	
Comprobaciones del historial personal	Se deben realizar comprobaciones del historial personal para descubrir cualquier problema posible, con objeto de reducir el riesgo al que se exponen la empresa y los empleados. Este proceso también permite localizar cualquier problema o laguna en el currículum del aspirante. El proceso de contratación de personal debe incluir una evaluación del historial laboral y cualquier antecedente penal del aspirante. Se deben evaluar las habilidades del aspirante comparándolas con las descripciones detalladas y los requisitos del puesto para detectar los puntos fuertes y débiles.	
	Resultados	**Recomendaciones**
Comprobaciones del historial personal	Su respuesta indica que en su empresa no se llevan a cabo comprobaciones del historial personal como parte integral del proceso de contratación.	Cree una directiva que requiera una comprobación del historial personal y financiero de las nuevas incorporaciones que vayan a ocupar puestos importantes. A la larga, esta directiva deberá englobar a todos los nuevos empleados, independientemente del puesto.
Subcategoría	**Mejores prácticas recomendadas**	
Directiva de recursos humanos	Los procedimientos formales para gestionar el caso de los empleados que dejan la empresa garantizan que se actúa debidamente cuando se rescinde un contrato de trabajo. Estos procedimientos deben existir para gestionar la situación de los empleados que dejan la empresa amistosamente y los que la dejan de forma hostil. Estos procedimientos deben incluir: + Notificación a todos los departamentos (Recursos humanos, TI, Seguridad física, Servicio de atención al cliente, Finanzas, etc.) + Acompañamiento del empleado al abandonar las instalaciones + Cancelación de todas las cuentas del usuario y de su acceso a la red + Recuperación de todos los bienes de la empresa (portátiles, PDA, dispositivos electrónicos, documentos confidenciales, etc.)	
	Resultados	**Recomendaciones**
Directiva de recursos humanos	Su respuesta indica que no existe ninguna directiva formal para los empleados que dejan la empresa.	Colabore con el departamento de recursos humanos para desarrollar de inmediato una directiva formal para los empleados que dejan la empresa. Contemple los supuestos de ceses amistosos y hostiles del puesto de trabajo. El aspecto más importante que se debe recoger en esta directiva es garantizar que ninguno de los empleados puede acceder físicamente a los recursos ni a los privilegios de TI una vez fuera de la empresa.
Subcategoría	**Mejores prácticas recomendadas**	
Relaciones con terceros	Con objeto de reducir el riesgo de revelación de datos, deben existir directivas y procedimientos formales enfocados a las relaciones con terceros. Así, se podrá detectar cualquier problema de seguridad y la responsabilidad de cada parte a la hora de solucionarlo. Estas directivas deben incluir:	

	+ El nivel de conectividad y acceso + La presentación y el tratamiento de los datos + Los roles y las responsabilidades (incluida la autoridad) de cada parte + La gestión de la relación: creación, mantenimiento y cese.	
	Resultados	**Recomendaciones**
Relaciones con terceros	Sus respuestas indican que los sistemas se configuran por parte de personal interno.	El personal interno debería configurar los sistemas siguiendo una simulación de creación.
Relaciones con terceros	Sus respuestas indican que su empresa gestiona el entorno informático.	Según las necesidades de la empresa, pueden ser soluciones viables tanto la gestión propia como la subcontratada. Si se subcontratan los servicios, los requisitos de seguridad deberían tratarse en el contrato y los acuerdos de nivel de servicio (SLA) deberían garantizar el cumplimiento de tales requisitos.
Relaciones con terceros	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise esta opción abierta con su personal de TI o con un socio de seguridad. Introduzca la respuesta más adecuada a esta pregunta en MSAT para obtener más información.

Tabla 19. Directiva y procedimientos

Tabla de Formación y conocimiento

Formación y conocimiento		
Subcategoría	**Mejores prácticas recomendadas**	
Conocimiento de seguridad	Un programa formal de divulgación de las medidas de seguridad ayuda a los empleados a contribuir a la seguridad global de la empresa, puesto que se les mantiene informado acerca de los riesgos existentes. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad. Un programa de divulgación efectivo debe tener en cuenta todos los aspectos de la seguridad (aplicaciones, redes y soportes físicos) y ofrecer también pautas claras a los empleados en caso de que detecten un riesgo para la seguridad de cualquiera de estos elementos. Ponga en práctica directivas para regular la utilización de los recursos corporativos por parte de los empleados. Los programas de divulgación deben formar parte del curso de orientación de empleados nuevos. Se debe proporcionar información actualizada y cursos para asegurar que todos los empleados conozcan las prácticas y los riesgos más recientes. Se deben realizar comprobaciones periódicas para asegurarse de que los empleados han asimilado la información.	
	Resultados	**Recomendaciones**
Conocimiento de seguridad	Sus respuestas indican que no ha asignado a ningún individuo ni grupo la seguridad de su empresa.	Nombre a una persona o grupo con experiencia en seguridad para que se responsabilice de la seguridad de la empresa y exija que se consulte a esta persona/equipo antes de que se realicen cambios en el entorno informático.
Conocimiento de seguridad	Su respuesta indica que no existe ningún programa de	Evalúe poner en práctica un programa formal de divulgación de seguridad para que los empleados

	divulgación de las medidas de seguridad en la empresa.	conozcan los riesgos relacionados con los recursos de TI. Ponga en práctica directivas que regulen la utilización de los recursos y las tecnologías corporativas por parte de los empleados e incluya un programa de divulgación de seguridad en el curso de orientación para nuevos empleados. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad.
Subcategoría	**Mejores prácticas recomendadas**	
Formación sobre seguridad	Trabaje con propietarios de empresa para determinar el tiempo de inactividad de aplicaciones críticas. Basándose en esos resultados, aplique las medidas oportunas para satisfacer e incluso superar esos requisitos. La disponibilidad y el rendimiento de las aplicaciones basadas en web mejoran al implementar equilibrio de carga delante de los servidores web. Para equilibrar la carga del servidor, el equilibrio de carga distribuye las solicitudes entre los distintos nodos en el clúster del servidor con el objetivo de optimizar el rendimiento del sistema. Si se produce un error en un servidor web en el clúster del servidor, la solicitud se dirige a otro servidor para atender la solicitud, lo que proporciona una alta disponibilidad. Determine el tiempo de inactividad aceptable para los usos compartidos de archivos y bases de datos de propietarios de empresa. Pruebe los mecanismos de conmutación por error para las aplicaciones y determine si la cantidad del tiempo de inactividad es aceptable.	
	Resultados	**Recomendaciones**
Formación sobre seguridad	Su respuesta indica que la empresa no ofrece actualmente a los empleados formación específica por temas.	En principio y según las exigencias de su modelo empresarial, desarrolle un plan para que el equipo de TI y de desarrollo tenga la formación de seguridad apropiada. Dé comienzo al plan garantizando la asistencia de este equipo a sesiones de formación como seminarios y foros específicos. Redacte el plan para que incluya cualquier tipo de curso básico para todos los empleados en el futuro.

Tabla 20. Formación y conocimiento

5.3.11. Lista de acciones recomendadas

La siguiente lista da prioridad a las recomendaciones presentadas anteriormente en la sección Detalles de la evaluación. Para obtener más información sobre cualquiera de estos elementos, consulte la entrada correspondiente en dicha sección.

Tabla de Lista de acciones recomendadas

Lista de acciones recomendadas	
Tema del análisis	***Recomendación***
Prioridad alta	
Infraestructura > Defensa del perímetro > Inalámbrico	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.
Infraestructura > Defensa del perímetro > Acceso remoto	Utilice VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH. Utilice conectividad sitio-a-sitio basada en la tecnología IPSec. Configure listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.
Personal > Directiva y procedimientos > Relaciones con terceros	El personal interno debería configurar los sistemas siguiendo una simulación de creación.
Aplicaciones > Implementación y uso > Aplicación y recuperación de datos	Todas las aplicaciones de líneas comerciales deberían evaluarse periódicamente para su seguridad, someterse a procesos regulares de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.
Infraestructura > Autenticación > Usuarios de acceso remoto	Además de permitir el acceso remoto a los empleados según las mejores prácticas recomendadas, considere limitar el acceso a los contratistas para que únicamente puedan acceder a los sistemas remotos necesarios. Por otro lado, plantéese utilizar un punto de entrada separado para los contratistas, con el fin de controlar y limitar su acceso con más facilidad.
Prioridad intermedia	
Infraestructura > Gestión y control > Seguridad física	Continúe utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.
Infraestructura > Autenticación > Cuentas inactivas	Visite con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus Realice auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas. Trabaje conforme a las mejores prácticas recomendadas.
Aplicaciones > Implementación y uso > Desarrollado internamente	No continúe utilizando macros de Office personalizadas, ya que es necesario que las configuraciones de seguridad de Office se reclasifiquen a un nivel inferior, por lo que sus aplicaciones ofimáticas quedan expuestas a documentos peligrosos.
Prioridad baja	
Infraestructura > Defensa del perímetro > Antivirus - Equipos de escritorio	Continúe con la práctica. Utilice una directiva que requiera a los usuarios a actualizar las firmas de virus. Piense en añadir el cliente antivirus al entorno predeterminado de creación de estaciones de trabajo.
Infraestructura > Defensa del perímetro > Antivirus - Servidores	Continúe con la práctica. Plantéese controlar activamente los clientes antivirus de los servidores desde una consola de gestión central para la utilización de configuraciones y firmas de virus. Si utiliza Microsoft Exchange, considere emplear las funciones adicionales de antivirus y los filtros de contenidos para los buzones de correo.
Aplicaciones > Diseño de aplicaciones > Autorización y control de acceso	Piense en probar exclusivamente las aplicaciones principales que procesen datos confidenciales y las interfaces disponibles para los usuarios por Internet. Incluya pruebas tipo "caja negra" e "informadas" de la aplicación y compruebe la asignación de mayores privilegios.

Tabla 21. Lista de acciones recomendadas

5.3.12. Apéndices

5.3.12.1. Preguntas y respuestas

Las siguientes respuestas se proporcionaron como entrada en esta evaluación.

Tabla de Preguntas y Respuestas

Cuestión de la evaluación	Su respuesta
Business Risk Profile	
Número de equipos de escritorio y portátiles que se utilizan en su empresa:	Entre 50 y 149
Número de servidores que se utilizan en su empresa:	Entre 1 y 5
¿Tiene su empresa una conexión permanente a Internet?	Sí
¿Acceden los clientes y fabricantes a su red o sistemas internos a través de Internet?	No
¿Alberga su empresa algunos servicios de aplicaciones externas, como por ejemplo, un portal o un sitio Web, para sus socios o clientes externos?	No
¿Dispone su empresa de servicios que usen los clientes internos y externos en el mismo segmento de red?	No
¿Se conectan directamente los socios o clientes externos a los sistemas internos de la aplicación para acceder a los datos, actualizar los registros o gestionar de cualquier otra forma la información?	No
¿Se utilizan los mismos componentes de infraestructura de aplicación, como por ejemplo, bases de datos en apoyo de las aplicaciones externas y los servicios corporativos internos?	No
¿Permite su empresa que los empleados o los contratistas accedan remotamente a la red corporativa interna?	Sí
¿Se permite que los empleados puedan utilizar sistemas que no sean de producción en la red corporativa general, como por ejemplo, servidores Web personales o equipos que actúen como hosts de "proyectos personales"?	No
Aparte de los dispositivos de cinta y de copia de seguridad, ¿permite su empresa procesar la información confidencial o de propiedad fuera de las instalaciones?	Sí
En el caso de que los sistemas de seguridad se vieran comprometidos, ¿afectaría ello significativamente la capacidad comercial de su empresa?	Sí
¿Comparte su empresa espacio de oficinas con otras entidades?	No
¿Se desarrollan aplicaciones en su empresa?	No
¿Permite su empresa que los desarrolladores de software se conecten de forma remota a los recursos de desarrollo corporativos o que desarrollen remotamente código para aplicaciones?	Sí

¿Desarrolla o pone en venta su empresa algunos productos de software para el uso de clientes, socios o el mercado en general?	No
¿Se permite que los desarrolladores prueben o desarrollen los sistemas en sitios remotos o inseguros?	No
¿Actúa el personal de TI como guardianes (en contraposición a los desarrolladores) de la línea de aplicaciones comerciales?	No
Según los procedimientos de su empresa, ¿es necesaria la actuación de un tercero para almacenar, procesar o distribuir los datos?	No
¿Se almacenan o procesan los datos del cliente en un entorno compartido con los recursos corporativos?	Sí
¿Recurre a fabricantes independientes de software para complementar la oferta de servicios empresariales?	No
¿Obtiene su empresa ingresos por ofrecer servicios que incluyen el procesamiento o la minería de datos?	No
Los datos que procesan las aplicaciones de su empresa, ¿se consideran confidenciales o vitales para las operaciones comerciales de sus clientes?	Sí
¿Se ofrecen aplicaciones comerciales críticas a través de conexiones a Internet?	No
¿Quiénes son los usuarios objetivos de las aplicaciones principales de su entorno?	Empleados internos
¿Cómo acceden los usuarios a las aplicaciones principales?	Solamente desde la red interna
¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?	No
¿Obtiene su empresa ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?	No
En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?	No
¿La actividad de su empresa depende de la recepción o el procesamiento de datos por parte de socios, fabricantes o terceros?	No
Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los clientes, como un apagón o el fallo de una aplicación o hardware, ¿afectaría significativamente a sus ingresos?	No
¿Almacena su empresa datos confidenciales de sus clientes o de importancia vital?	Sí
Los componentes de infraestructura y las aplicaciones del cliente, ¿dependen del acceso a recursos de su entorno?	No
¿Comparte su empresa los componentes de infraestructura y aplicaciones entre varios clientes?	No
¿Considera que los recursos de TI son un requisito para su empresa?	Sí
¿Utilizan todos los empleados de su empresa equipos informáticos para desarrollar su trabajo?	No
¿Subcontrata su empresa el mantenimiento o la propiedad de alguna parte de su infraestructura?	Sí
¿Tiene su empresa algún plan a medio o largo plazo para la selección y utilización de componentes de nuevas tecnologías?	No
¿Cree que su empresa participa en la adopción rápida de las nuevas tecnologías?	No

¿Selecciona e implanta su empresa nuevas tecnologías basadas en acuerdos de licencias y asociaciones existentes?	No
¿Limita su empresa las opciones relacionadas con la tecnología a aquellas que conoce actualmente el personal de TI?	Sí
¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?	No
¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo datos corporativos o datos confidenciales de los clientes?	No
¿Limita su empresa el acceso a la información en función de los roles de los usuarios?	Sí
¿Implanta su empresa nuevos servicios o aplicaciones antes de evaluar los posibles riesgos para la seguridad?	No
¿Cambia su empresa periódicamente las credenciales de las cuentas con privilegios?	No
¿Cambia su empresa las credenciales de las cuentas con privilegios cuando el personal deja de trabajar en la empresa?	Sí
Seleccione la opción que mejor defina el sector profesional de su empresa:	Otro
Seleccione el número de empleados de su empresa:	Entre 50 y 149 empleados
¿Su empresa tiene más de una oficina?	No
¿La actividad de su empresa se desarrolla en un mercado de gran competencia o de investigación, en el que el robo de material intelectual o el espionaje son temas de gran preocupación?	No
¿Cambia muy a menudo el personal técnico en su empresa?	No
¿Los productos o las marcas de su empresa tienen reconocimiento?	No
¿Utiliza su empresa versiones obsoletas de software que ya no cuenten con el servicio técnico del fabricante?	No
¿Adquiere su empresa el software de fabricantes o proveedores conocidos y fiables?	Sí
Infraestructura	
¿Utiliza su empresa cortafuegos u otros controles de acceso en los perímetros de la red para proteger los recursos corporativos?	No
¿Alberga su empresa servicios relacionados con Internet en la red corporativa?	No
¿Utiliza su empresa software de cortafuegos basado en hosts para proteger los servidores?	No
¿Utiliza su empresa hardware o software de detección de intrusiones para identificar los ataques a la seguridad?	No
¿Se utilizan soluciones antivirus en el entorno?	Sí
Seleccione los sistemas que utilizan soluciones antivirus:	Equipos de escritorio Servidores
¿Se puede acceder a la red de la empresa de forma remota?	Sí
Seleccione quién se puede conectar a la red de forma remota:	Contratistas
¿Se utiliza la tecnología de red privada virtual (VPN) para la conectividad segura a los recursos corporativos de los usuarios remotos?	No

¿Se utiliza autenticación multifactor (token o tarjeta inteligente, etc.) para los usuarios remotos?	No
¿Tiene la red más de un segmento?	No
¿Dispone la red de opciones de conexión inalámbrica?	Sí
¿Cuáles de los siguientes controles de seguridad se usan para regular las conexiones a las redes inalámbricas?	Activar Acceso protegido de fidelidad inalámbrica (WPA)
¿Existen controles para hacer cumplir las directivas de contraseñas en todas las cuentas?	No
¿Su organización dispone de procesos para revisar cuentas administrativas inactivas, de uso interno, de proveedor y de usuario remoto?	No
¿Es su empresa la que configura los sistemas o esta tarea la efectúan otros proveedores o revendedores de hardware?	Configurado por personal interno
¿Cuáles de los siguientes elementos se han creado basándose en una configuración documentada o en una simulación formal?	Ninguno
¿Cuáles de las soluciones siguientes se han instalado en las estaciones de trabajo y los portátiles de los empleados?	Software de gestión/control remoto
¿Su organización cuenta con procedimientos de respuesta ante incidentes formales?	No
¿Se han aplicado controles de seguridad físicos para garantizar la seguridad de los activos de la empresa?	Sí
¿Cuáles de los siguientes controles de seguridad se utilizan?	Equipos de red (conmutadores, cableado, conexión a Internet) en habitaciones cerradas con acceso restringido Los equipos de red se encuentran además en un armario cerrado Los servidores están en una habitación cerrada con acceso restringido
¿Cuáles de los siguientes controles de acceso físico se utilizan?	Registros de visitantes
Aplicaciones	
¿Dispone su empresa de una línea de aplicaciones comerciales (LOB)?	Sí
¿Utiliza macros personalizadas para las aplicaciones de Office (como, por ejemplo, Word, Excel o Access)?	No
¿Qué mecanismos tiene su empresa para asegurar una disponibilidad alta de las aplicaciones? Seleccione los mecanismos utilizados de la lista siguiente:	Ninguno
¿Ha desarrollado un equipo interno de desarrollo algunas de las aplicaciones principales de su entorno?	No
¿Los consultores/proveedores de terceros han desarrollado alguna aplicación clave implementada en su entorno?	No
¿Qué metodologías de desarrollo de seguridad de software se practican en su empresa? (Seleccione todas las respuestas que correspondan)	Ninguna
¿Conoce su empresa las vulnerabilidades de seguridad que existen actualmente en las aplicaciones de su entorno?	No
¿Su empresa proporciona formación sobre seguridad para el personal de desarrollo y pruebas?	No

¿Su empresa confía en herramientas de software como parte del proceso de prueba y auditoría para el desarrollo de software seguro?	No
¿Existen controles para hacer cumplir las directivas de contraseñas de las aplicaciones principales?	No
¿Tienen las aplicaciones principales del entorno mecanismos para limitar el acceso a los datos y las funciones confidenciales?	Sí
¿Guardan las aplicaciones principales del entorno mensajes en archivos de registro para su análisis y auditoría?	No lo sé.
¿Las aplicaciones utilizadas validan los datos de entrada?	No lo sé.
¿Cifran las aplicaciones principales los datos confidenciales y críticos de la empresa que se encargan de procesar?	No
Operaciones	
¿Es la empresa la que gestiona el entorno o se contrata los servicios de un tercero?	La empresa gestiona el entorno
¿Utiliza la empresa hosts de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?	No
¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las actividades administrativas o de gestión?	No
¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?	Sí
¿Se comprueba periódicamente el cortafuego para garantizar que funciona según lo previsto?	No
¿Su organización mantiene planes de recuperación ante desastres y de reanudación de negocio?	No
¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?	No
¿Existen directivas para la regulación del entorno informático?	No
¿Hay un proceso documentado para la creación de hosts? Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de hosts hay un proceso de creación documentado?)	Ninguno
¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:	No hay directivas
¿Su organización dispone de un proceso formal bien documentado para la eliminación de datos en medios electrónicos y en formato impreso?	No
¿Su organización dispone de un esquema de clasificación de datos con directrices de protección de datos asociadas?	No
¿Hay un proceso de gestión para las configuraciones y los cambios?	No
¿Existe un proceso establecido para las directivas de actualización y revisión?	No
¿Existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas?	Antivirus
¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los hosts?	No
¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?	No
¿Está activado en el entorno el registro de los eventos producidos en los hosts y los dispositivos?	No

¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?	No
Personal	
¿Hay en su empresa individuos o grupos que sean responsables de la seguridad?	No
¿Realiza su empresa evaluaciones de la seguridad del entorno a través de terceros?	No
¿Realiza su empresa evaluaciones de la seguridad del entorno de forma interna?	No
¿Realiza la empresa comprobaciones del historial personal como parte del proceso de contratación?	No
¿Hay un proceso formal para la salida de la empresa de los empleados?	No
¿Hay una directiva formal para las relaciones con terceros?	No lo sé.
¿Hay un programa de divulgación de las medidas de seguridad en su empresa?	No
¿Se ofrece a los empleados formación relacionada con el cargo que desempeñan en la empresa?	No

Tabla 22. Preguntas y Respuestas

5.3.12.2. Glosario

El glosario presenta los términos y conceptos estándar en el sector de las soluciones de seguridad mencionados en este informe. También se pueden incluir términos adicionales que no se encuentran en este informe.

Tabla de Glosario

Término	Definición
AoAs	Áreas de análisis que son la infraestructura, las aplicaciones, operaciones, y la gente.
Aplicaciones	Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que ejecutarse. Algunos ejemplos son los procesadores de texto, las hojas de cálculo o los programas de gestión de bases de datos.
Antivirus (AV)	Software o tecnología de hardware que protege al entorno informático frente a cualquier software peligroso.
Perfil de riesgos para la empresa (BRP)	Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.
Índice de defensa en profundidad (DiDl)	Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.
Zona desmilitarizada	Parte de la red separada de la red interna mediante un cortafuegos y

(DMZ)	conectada a Internet a través de otro cortafuegos.
Servidor de seguridad (cortafuegos)	Dispositivo de hardware o software que ofrece protección a los equipos frente al acceso no autorizado a través de la red.
Infraestructura	Funcionalidad de red, así como su administración y mantenimiento para ofrecer compatibilidad con la defensa de red, respuesta frente a incidentes, disponibilidad de red y análisis de errores. Incluye compatibilidad con los procesos empresariales internos y externos, y acerca de cómo se crean e implementan los hosts.
Autenticación multifactor	Autenticación que requiere una combinación de al menos dos de los siguientes elementos: algo que se sabe; algo que se tiene; o algo propio del usuario. Por ejemplo, la tarjeta de débito de su banco es una autenticación de dos factores: requiere algo que tiene (la tarjeta) y algo que sabe (el número PIN). Solicitar a alguien que teclee múltiples contraseñas para la autenticación, supone una autenticación de un solo factor al tratarse únicamente de algo que sabe el usuario. Por lo general, cuantos más factores, más segura es la autenticación. Así, un sistema que requiera un tarjeta identificativa (algo que posee), un PIN (algo que sabe) y una huella dactilar escaneada (algo propio) es más seguro que cualquier otro que únicamente solicite el nombre de usuario/contraseña (factor único) o una tarjeta de identidad y el PIN.
Operaciones	The policies, processes, procedures, and practices related to the protection
Personal	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Infraestructura de clave pública (PKI)	Conjunto integrado de tecnologías necesario para proporcionar un cifrado por clave pública y firmas digitales. Utiliza una combinación de cifrado por clave pública y privada que ofrece gestión de claves e integridad y confidencialidad de los datos.
Proceso	Serie documentada de tareas secuenciales que se utiliza para realizar una función del negocio.

Tabla 23. Glosario

5.3.13. Interpretación de gráficos

- La puntuación del BRP va de 0 a 100. Una puntuación más alta significa un riesgo posible aumentado al que está expuesta su empresa en esta área de análisis. Es importante tener en cuenta que una puntuación de 0 no es posible; dedicarse a una actividad comercial siempre implica un nivel de riesgo. También es importante comprender que hay riesgos comerciales que no se pueden mitigar directamente.

- DiDI también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde han tomado más medidas para implementar estrategias de DiD en el área de análisis específica. La puntuación DiDI no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

- En principio, una puntuación baja del BRP y alta del DiDI parecería un buen resultado, pero no siempre es así. Está fuera del ámbito de la presente autoevaluación tener en cuenta todos los factores. Una disparidad significativa entre la puntuación del BRP y la del DiDI para un área de análisis específica significa que se recomienda una revisión del área. Cuando analice sus resultados, es importante tener en cuenta las puntuaciones individuales, tanto de BRP como de DiDI, y cómo se relacionan entre sí. Un entorno estable probablemente tendría como resultado puntuaciones iguales en todas las áreas. Disparidades entre las puntuaciones DiDI son un indicio de una estrategia general de seguridad concentrada en una sola técnica de mitigación. Si la estrategia de seguridad no abarca el personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque.

5. CAPITULO II. DISEÑO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICADA A E.S.E. HOSPITAL SAN NICOLÁS.

5.3. Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de

directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la Empresa Social del Estado Hospital San Nicolás.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propensa la E.S.E. Hospital San Nicolás, surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a la E.S.E. Hospital San Nicolás.

5.4. Alcance de Las Políticas

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y de vulnerabilidades en las dependencias de la E.S.E. Hospital San Nicolás, por consiguiente el alcance de estas políticas, se encuentra sujeto a la empresa.

5.5. Objetivo de las Políticas

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa".

Los objetivos que se desean alcanzar luego de implantar nuestro sistema de seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de la E.S.E. Hospital San Nicolás en la administración del riesgo.
- Comprometer todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Garantizar que la prestación del servicio de seguridad gane en calidad.
- Involucrar todos los empleados para que se conviertan en interventores del sistema de seguridad.

5.6. Análisis de las razones que impiden la aplicación de las Políticas de seguridad informática.

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que quienes toman las

decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la empresa.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la empresa, ellas deben responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la empresa.

5.7. Responsabilidades

Es responsabilidad del supervisor de Seguridad Informática, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, revistas internas) de los Procedimientos de Seguridad. Asimismo, es responsabilidad del supervisor inmediato capacitar a sus empleados en lo relacionado con los Procedimientos de Seguridad.

5.8. Definición de Políticas de Seguridad Informática

En esta sección del documento se presenta una propuesta de políticas de seguridad, como un recurso para mitigar los riesgos a los que la E.S.E. Hospital San Nicolás. Se ve expuesta.

5.9. Disposiciones Generales

Artículo 1°.- El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la Empresa Social del Estado Hospital San Nicolás.

Artículo 2°.- Para los efectos de este instrumento se entenderá por:

5.9.2. Comité

Al equipo integrado por la Gerencia, los Jefes de área y el personal administrativo (ocasionalmente) convocado para fines específicos como:

- Adquisiciones de Hardware y software.
- Establecimiento de estándares de la E.S.E. Hospital San Nicolás tanto de hardware como de software.
- Establecimiento de la Arquitectura tecnológica de grupo.
- Establecimiento de lineamientos para concursos de ofertas.

5.9.3. Administración de informática

Está integrada por la Gerencia y Jefes de área, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Elaborar y efectuar seguimiento del Plan Maestro de Informática.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Mantener la Arquitectura tecnológica.
- Controlar la calidad del servicio brindado.
- Mantener el Inventario actualizado de los recursos informáticos.
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

Artículo 3°.- Para los efectos de este documento, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben observar los Jefes de Sistemas responsables del hardware y software existente en la E.S.E. Hospital San Nicolás, siendo responsabilidad de la Administración de Informática, vigilar su estricta

observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Artículo 4°.- Las Políticas en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo de la E.S.E. Hospital San Nicolás. Estas normas inciden en la adquisición y el uso de los Bienes y Servicios Informáticos, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.

Artículo 5°.- La instancia rectora de los sistemas de informática de la E.S.E. Hospital San Nicolás es la Gerencia, y el organismo competente para la aplicación de este ordenamiento, es el Comité.

Artículo 6°.- Las Políticas aquí contenidas, son de observancia para la adquisición y uso de bienes y servicios informáticos, en la E.S.E. Hospital San Nicolás, cuyo incumplimiento generará que se incurra en responsabilidad administrativa; sujetándose a lo dispuesto en la sección Responsabilidades Administrativas de Sistemas.

Artículo 7°.- La E.S.E. Hospital San Nicolás deberá contar con un Jefe o responsable, en el que recaiga la administración de los Bienes y Servicios, que vigilará la correcta aplicación de los ordenamientos establecidos por el Comité y demás disposiciones aplicables.

5.9.4. Lineamientos para la adquisición de bienes informáticos

Artículo 8°.- Toda adquisición de tecnología informática se efectuará a través del Comité, que está conformado por el personal de la Administración de Informática.

Artículo 9°.- La adquisición de Bienes de Informática en la E.S.E. Hospital San Nicolás, quedará sujeta a los lineamientos establecidos en este documento.

Artículo 10°.- La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

5.9.5. Precio.

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

5.9.6. Calidad

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

5.9.7. Experiencia

Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

5.9.8. Desarrollo Tecnológico

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

5.9.9. Estándares

Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

5.9.10. Capacidades

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Artículo 11°.- Para la adquisición de Hardware se observará lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la E.S.E. Hospital San Nicolás.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática de la E.S.E. Hospital San Nicolás, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigente en el mercado y en la E.S.E. Hospital San Nicolás, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores de medios (HUBS) y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones al vencer su período de garantía.

- En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.

Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Comité.

Artículo 12°.- En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones del artículo siguiente.

Artículo 13°.- Para la adquisición de Software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectivos.

Artículo 14°.- Todos los productos de Software que se utilicen a partir de la fecha en que entre en vigor el presente ordenamiento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con el debido licenciamiento.

Artículo 15°.- Para la operación del software de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información institucional deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los sistemas de información, deberá contar con los privilegios ó niveles de seguridad de acceso suficientes para garantizar la seguridad total de la

información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CDs de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, la Unidad de Informática recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

Artículo 16°.- Para la prestación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:

Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.

5.9.11. Instalaciones de los equipos de cómputo

Artículo 17°.- La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- La Administración de Informática, así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencias fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios. En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

Artículo 18°.- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

5.9.12. Lineamientos en Informática: Información

Artículo 19°.- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:

- Información histórica para auditorias.
- Información de interés de la Empresa
- Información de interés exclusivo de alguna área en particular.

Artículo 20°.- Los jefes de área responsables de la información contenida en los departamentos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Artículo 21°.- Se establecen tres tipos de prioridad para la información:

- Información vital para el funcionamiento del área;
- Información necesaria, pero no indispensable en el área.
- Información ocasional o eventual.

Artículo 22°.- En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

Artículo 23°.- La información necesaria pero no indispensable, deberá ser respaldado con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

Artículo 24°.- El respaldo de la información ocasional o eventual queda a criterio del área.

Artículo 25°.- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento. Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.

Artículo 26°.- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

Artículo 27°.- Ningún colaborador en proyectos y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial de la E.S.E. Hospital San Nicolás tanto ahora como en el futuro.

5.9.13. Funcionamiento de los equipos de cómputo

Artículo 28°.- Es obligación de la Administración de Informática vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Artículo 29°.- Los colaboradores de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

Artículo 30°.- Por seguridad de los recursos informáticos se deben establecer seguridades:

- Físicas
- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.

- Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento.

Artículo 31°.- En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad de la E.S.E. Hospital San Nicolás, excepto en casos emergentes que la Dirección autorice.

5.9.14. Plan de contingencias informáticas

Artículo 32°.- La Administración de Informática creará para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

5.9.15. Estrategias informáticas

Artículo 33°.- La estrategia informática de la E.S.E. Hospital San Nicolás se consolida en el Plan Maestro de Informática y está orientada hacia los siguientes puntos:

- Plataforma de Sistemas Abiertos (Portables).
- Esquemas de operación bajo el concepto multicapas.
- Estandarización de hardware, software base, utilitarios y estructuras de datos
- Intercambio de experiencias entre Departamentos.
- Manejo de proyectos conjuntos con las diferentes áreas.
- Programa de capacitación permanente para los colaboradores de la empresa.

Artículo 34°.- Para la elaboración de los proyectos informáticos y para la presupuestario de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con los que cuente la E.S.E. Hospital San Nicolás.

5.9.16. Acceso Físico

Artículo 35°.- Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial de la E.S.E. Hospital San Nicolás.

Artículo 36°.- Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

5.9.17. Identificadores de usuario y contraseñas

Artículo 37°.- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Artículo 38°.- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Artículo 39°.- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

Artículo 40°.- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Artículo 41°.- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

5.9.18. Responsabilidades Personales

Artículo 42°.- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Artículo 43°.- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Artículo 44°.- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 45°.- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

Artículo 46°.- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

Artículo 47°.- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

Artículo 48°.- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

Artículo 49°.- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Artículo 50°.- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Artículo 51°.- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Artículo 52°.- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Artículo 53°.- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Artículo 54°.- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Artículo 55°.- Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Artículo 56°.- Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo en Outlook)

5.9.19. Salida de Información

Artículo 57°.- Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

Artículo 58°.- Además, en la salida de datos especialmente protegidos (como son los datos de carácter personal para los que el Reglamento requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro

mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

5.9.20. Uso apropiado de los recursos

Artículo 57°.- Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

5.9.21. Queda Prohibido

Artículo 58°.- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Artículo 59°.- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la E.S.E. Hospital San Nicolás.

Artículo 60°.-Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

Artículo 61°.- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por SASF tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Artículo 62°.- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Artículo 63°.- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Artículo 64°.- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

5.9.22. Software

Artículo 65°.- Todo el personal que accede a los Sistemas de Información de la E.S.E. Hospital San Nicolás debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Artículo 66°.-Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

Artículo 67°.-También tiene prohibido borrar cualquiera de los programas instalados legalmente.

5.9.23. Recursos de red

De forma rigurosa, ninguna persona debe:

Artículo 68°.- Conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones (Ej. módem) que posibilite la conexión a la Red Corporativa.

Artículo 69°.- Conectarse a la Red Corporativa a través de otros medios que no sean los definidos.

Artículo 70°.- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Artículo 71°.- Intentar acceder a áreas restringidas de los Sistemas de Información o de la Red Corporativa.

Artículo 72°.- Intentar distorsionar o falsear los registros “log” de los Sistemas de Información.

Artículo 73°.- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

Artículo 74°.- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

5.9.24. Conectividad a internet

Artículo 75°.- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la E.S.E. Hospital San Nicolás tienen las mismas responsabilidades en cuanto al uso de Internet.

Artículo 76°.- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Artículo 77°.- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Artículo 78°.- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Artículo 79°.- En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.

5.9.25. Actualizaciones de la política de seguridad

Artículo 80°.- Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la E.S.E. Hospital San Nicolás se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los colaboradores de la E.S.E. Hospital San Nicolás.

Artículo 81°.- Es responsabilidad de cada uno de los colaboradores de la E.S.E. Hospital San Nicolás la lectura y conocimiento de la Política de Seguridad más reciente.

5.9.26. Disposiciones Transitorias

Artículo primero.- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su difusión.

Artículo segundo.- Las normas y políticas objeto de este documento, podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité Técnico de Informática de la E.S.E. Hospital San Nicolás una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

Artículo tercero.- Las disposiciones aquí descritas constarán de forma detallada en los manuales de políticas y procedimientos específicos.

Artículo cuarto.- La falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

5.9.27. Beneficios de implantar políticas de seguridad informática

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que la E.S.E. Hospital San Nicolás trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los Recursos Humanos.

6. CAPITULO III. IMPLEMENTACIÓN EN SERVIDORES VIRTUALES DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA GESTIÓN Y ADMINISTRACIÓN DE LA RED DE DATOS DE E.S.E. HOSPITAL SAN NICOLÁS.

En este capítulo se diseñó un modelo de seguridad de la información para suplir los requerimientos de seguridad en la red del Hospital San Nicolás de Planeta rica, para esto se simuló la implementación de un firewall en software libre llamado Endian UTM, al cual se le configuraron las políticas de ruteo entre las diferentes zonas (Verde: LAN, Roja: Internet, Naranja: DMZ), el proxy, el IPS, IDS, antivirus y demás servicios necesarios para su óptimo funcionamiento de acuerdo a las necesidades planteadas.

Cada una de las anteriores configuraciones será explicada en detalle al momento de la implementación.

6.1. Nuevo escenario de la red de datos del Hospital San Nicolás de planeta Rica.

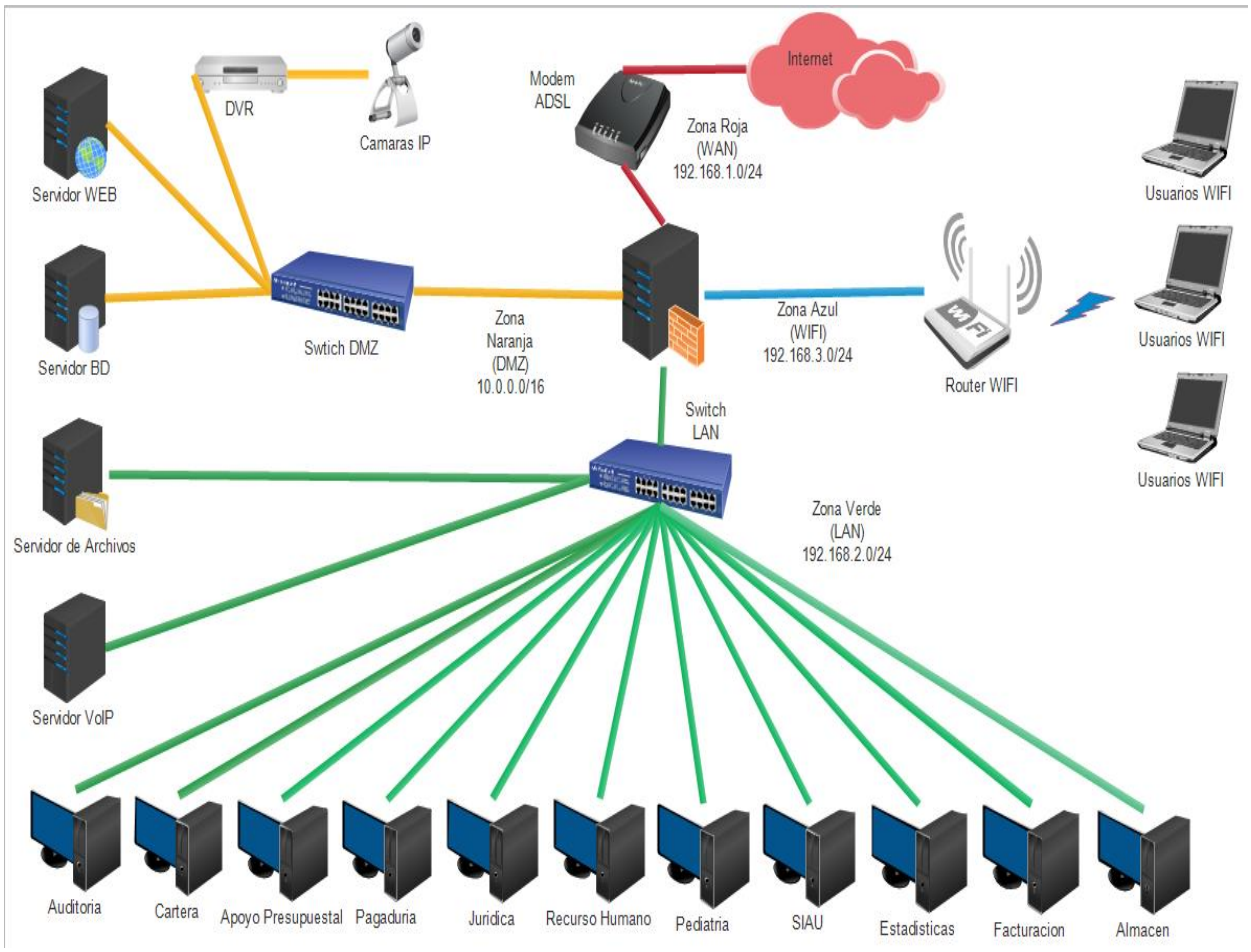

Ilustración 6. Nuevo escenario de la red del Hospital San Nicolás de Planeta Rica

6.2. Manual de Instalación y configuración de Endian Firewall UTM

Antes de comenzar con la instalación debemos descargar la ISO de Endian (http://www.endian.com/), después quemamos la ISO y la insertamos en nuestro servidor y booteamos. Comenzamos la instalación, podemos dar enter directamente o esperar unos segundos para que arranque el wizard de Instalación. Después de este nos salta una imagen donde elegimos el idioma.

Ilustración 7. Selección del idioma

A continuación nos mostrara un mensaje de bienvenida para la instalación de Endian.

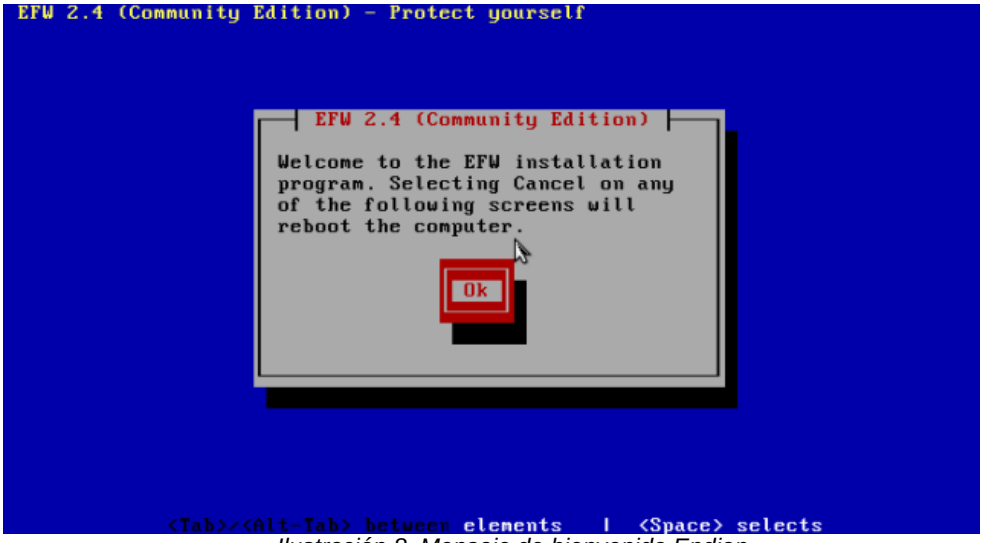

Ilustración 8. Mensaje de bienvenida Endian

Después nos aparecerá una advertencia, la cual especifica que el proceso de

instalación borrara todos los datos que contenga el disco duro, si deseamos continuar seleccionamos YES

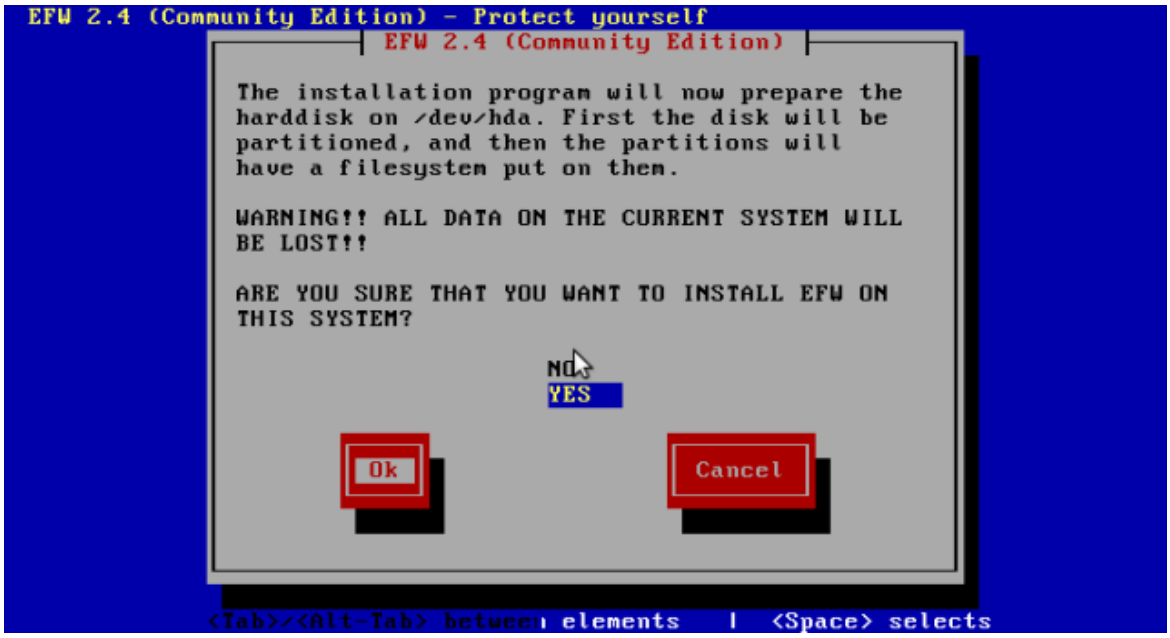

Ilustración 9. Formateo del disco

La siguiente pantalla nos ofrece la posibilidad de activar el servicio de Consola, esta opción la debemos elegir según nuestras necesidades.

Ilustración 10. Activar servicios de consola

Ahora Endian comenzara a instalarse en nuestro disco duro, y podemos ver que nos

irán saliendo mensajes como los siguientes.

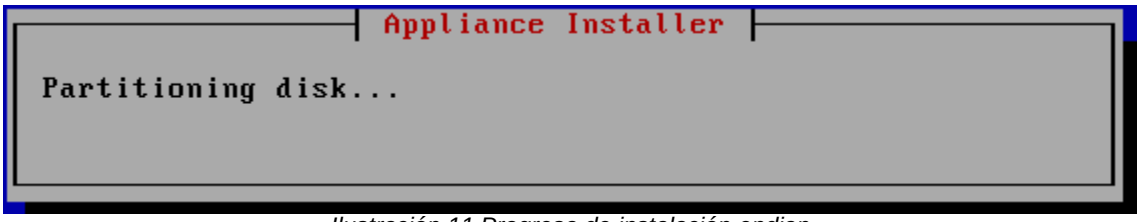

Ilustración 11.Progreso de instalación endian

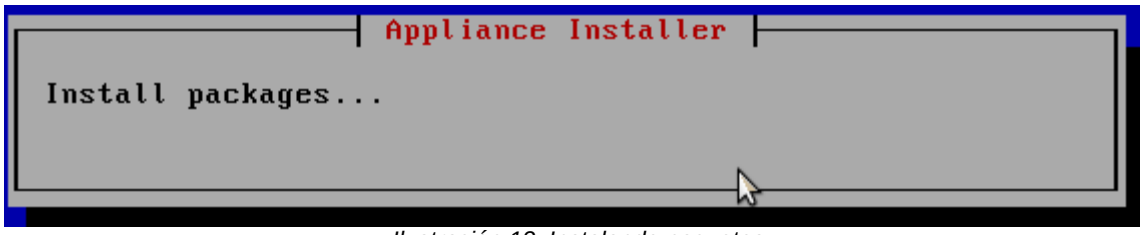

Ilustración 12. Instalando paquetes

Después del proceso de instalación, nos aparecerá una pantalla en la cual debemos de configurar la dirección IP de la interfaz de red local (GREEN) para posteriores configuraciones de Endian mediante el navegador web. En nuestro caso la dirección IP es la 192.168.2.1 con mascara de subred 255.255.255.0

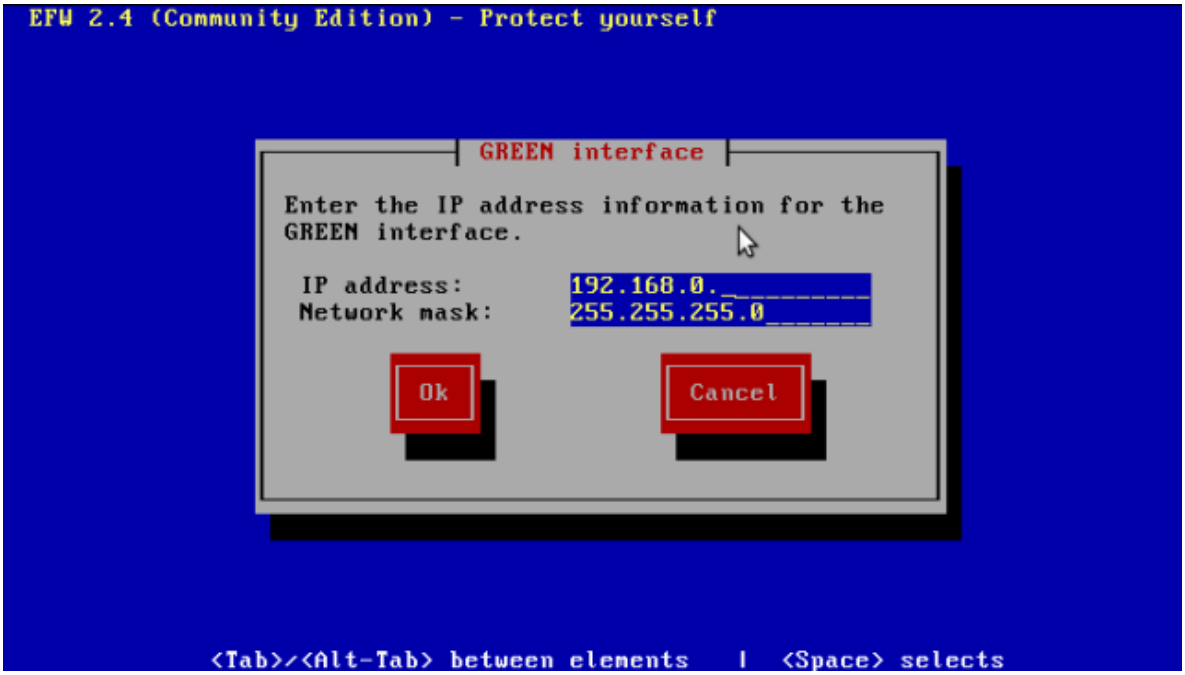

Ilustración 13. Configuración IP

Para finalizar el proceso de instalación, se nos recomienda quitar cualquier diskette o CD-ROM que aún se encuentre insertado, damos OK para que el sistema se reinicie.

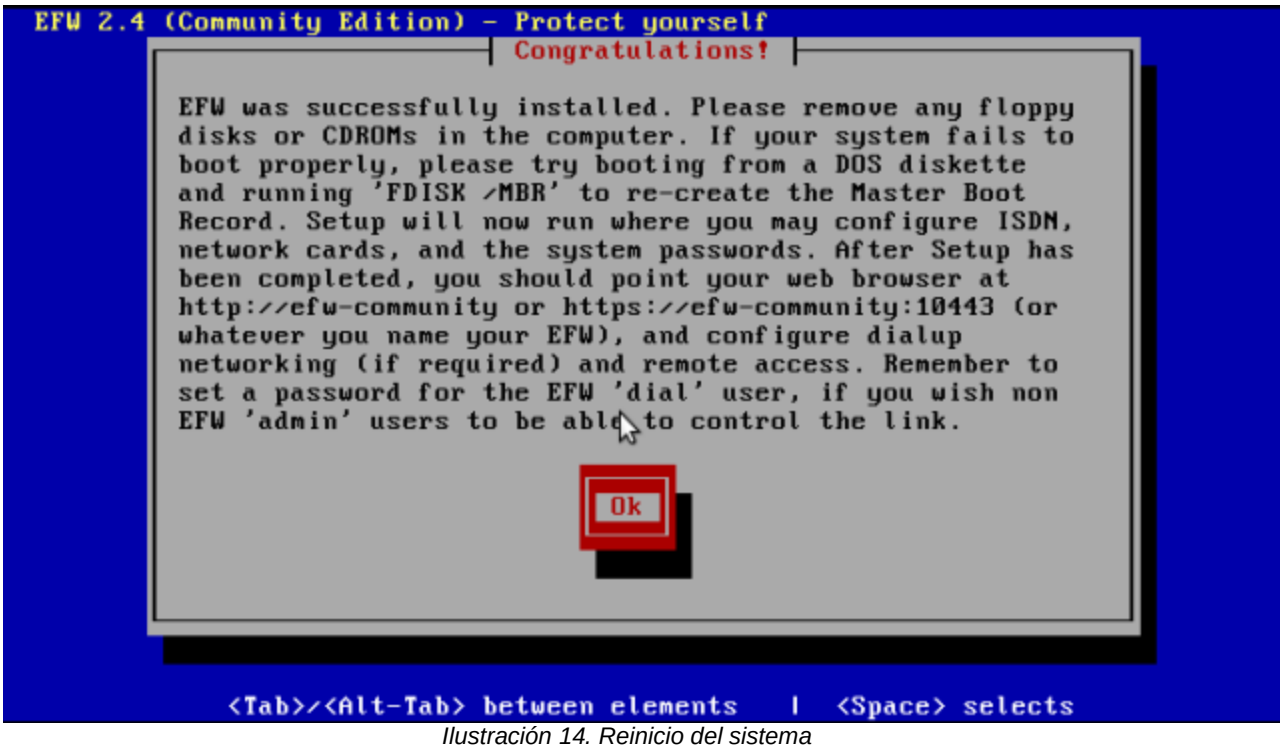

Ilustración 14. Reinicio del sistema

Después de que Endian se reinicie por completo nos aparecerá la siguiente pantalla en la cual podemos elegir las diferentes opciones según nuestro criterio. Una vez hechos estos pasos empezaremos la configuración. Nota: la contraseña del root es Endian y la Green IP es 192.168.2.1.

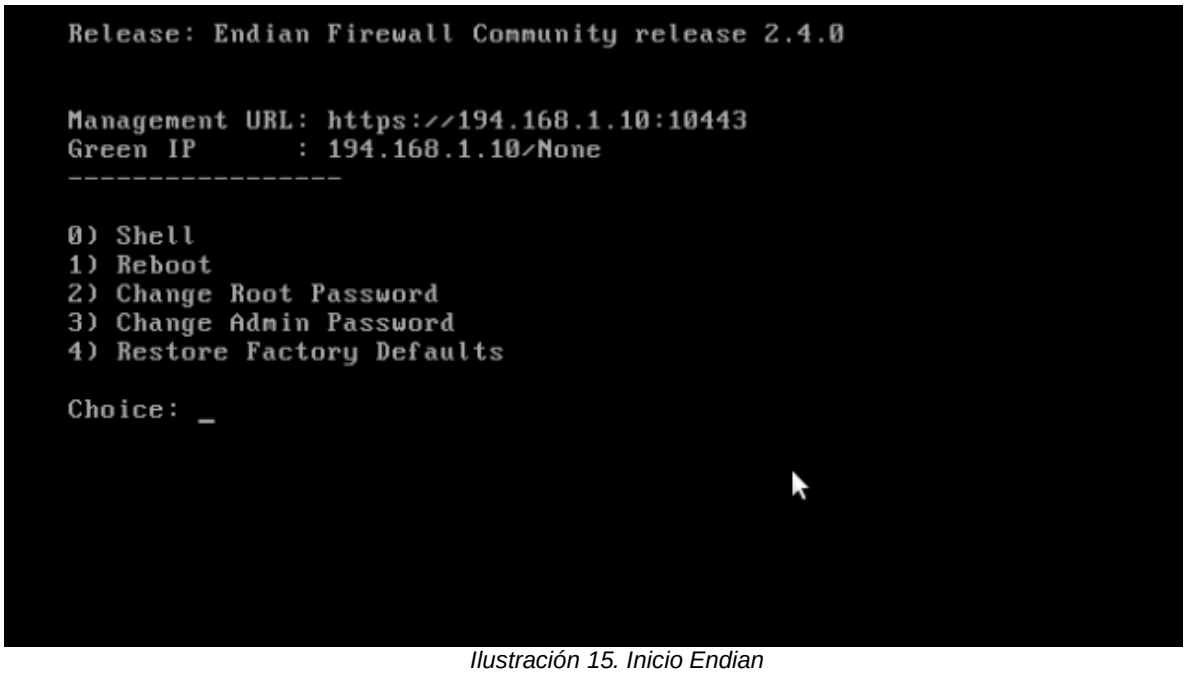

Ilustración 15. Inicio Endian

Cuando nos aparezca este pantallazo escogeremos la opción 0 para ingresar a la

Shell. Una vez allí le diremos login y pondremos la contraseña del root que por defecto es endian. Aquí podremos administrar desde la Shell de endian con algunos de los comandos que usualmente usamos en nuestras maquina con SO en Linux.

Con un PC que se encuentre dentro del mismo rango de direcciones, abrimos un navegador web y escribimos la dirección la IP que le asignamos al servidor Endian para acceder a panel web https://192.168.2.1:10443.

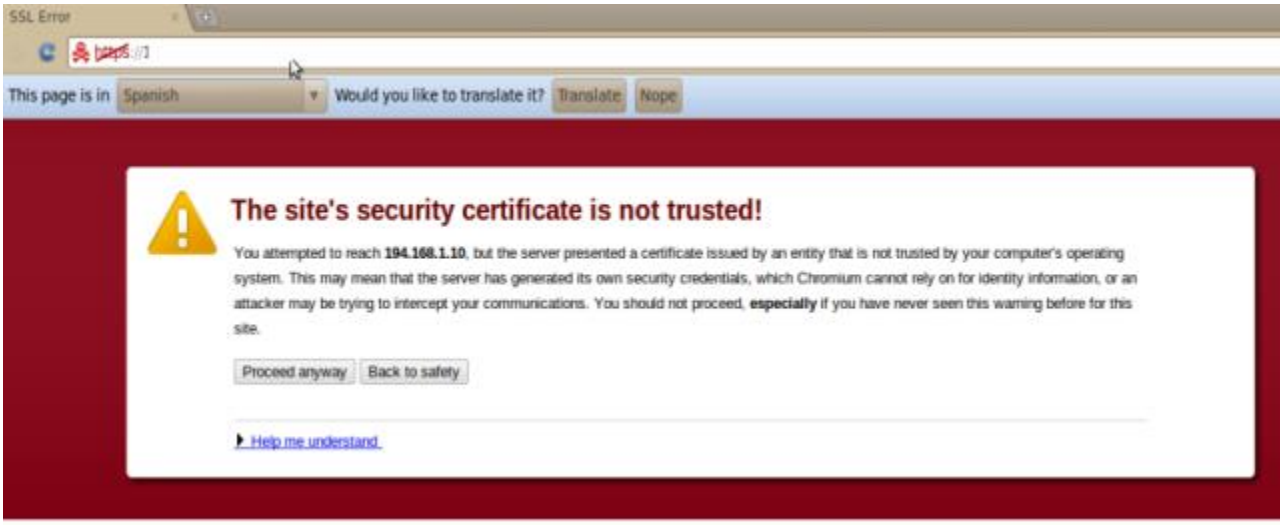

Ilustración 16. Verificación de IP

Aceptamos la validación del certificado de la interfaz web de Endian, para que podamos acceder a la configuración básica de Endian.

A continuación aparecerá la bienvenida a la configuración de Endian. Para continuar damos clic en el botón con las flechas (siguiente). >>>

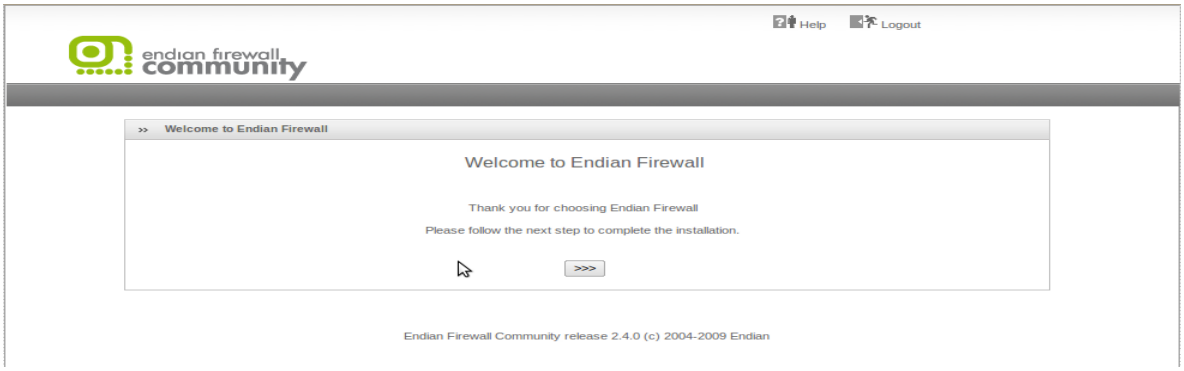

Ilustración 17. Bienvenida de Endian

Ahora vamos a escoger el idioma con el cual queremos configurar Endian, también

tenemos la opción de configurar la zona horaria según nuestra ubicación.

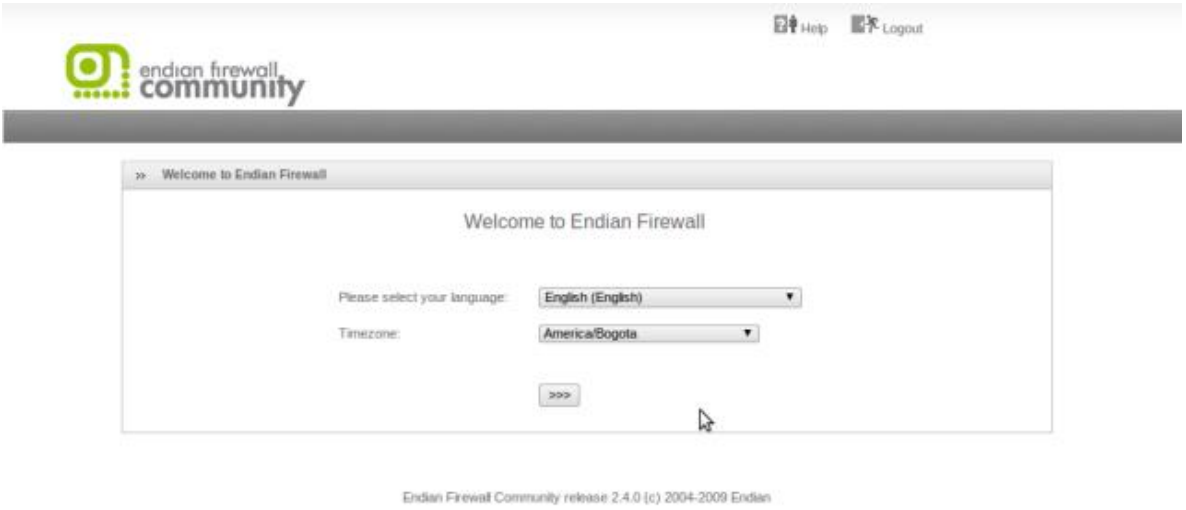

Ilustración 18. Selección de idioma de configuración Endian

Aceptamos el acuerdo de licencia sobre el uso de Endian

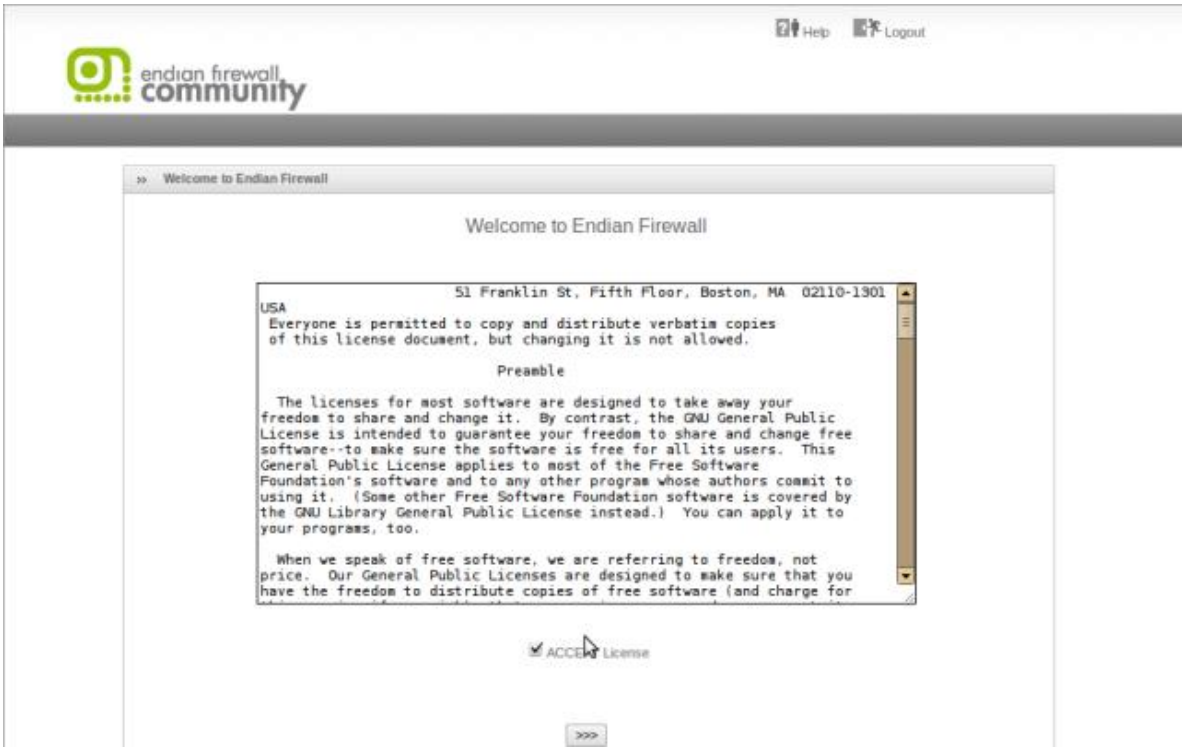

Ilustración 19. Licencia de uso Endian

Endian ahora nos pregunta que si queremos restablecer la configuración desde un archivo de respaldo o backup, pero como es primera vez que lo instalamos entonces dejemos la opción no y continuamos.

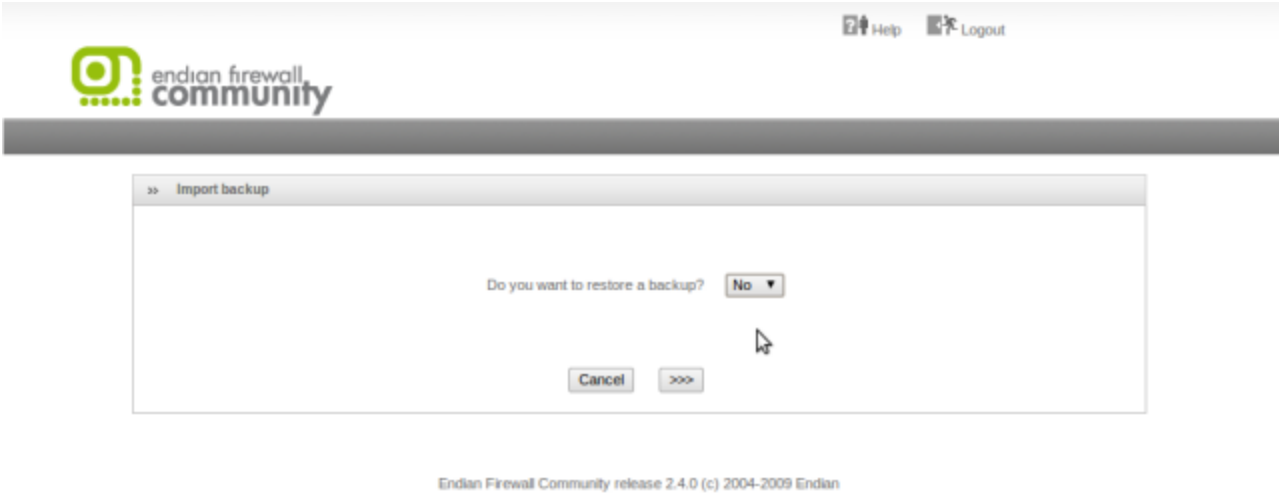

Ilustración 20. Restablecer configuración Endian

En la siguiente pantalla debemos configurar las contraseñas para la administración de la interfaz web y del usuario root, cabe recalcar que entre más seguras sea nuestra contraseña más difícil le hacemos el trabajo al atacante.

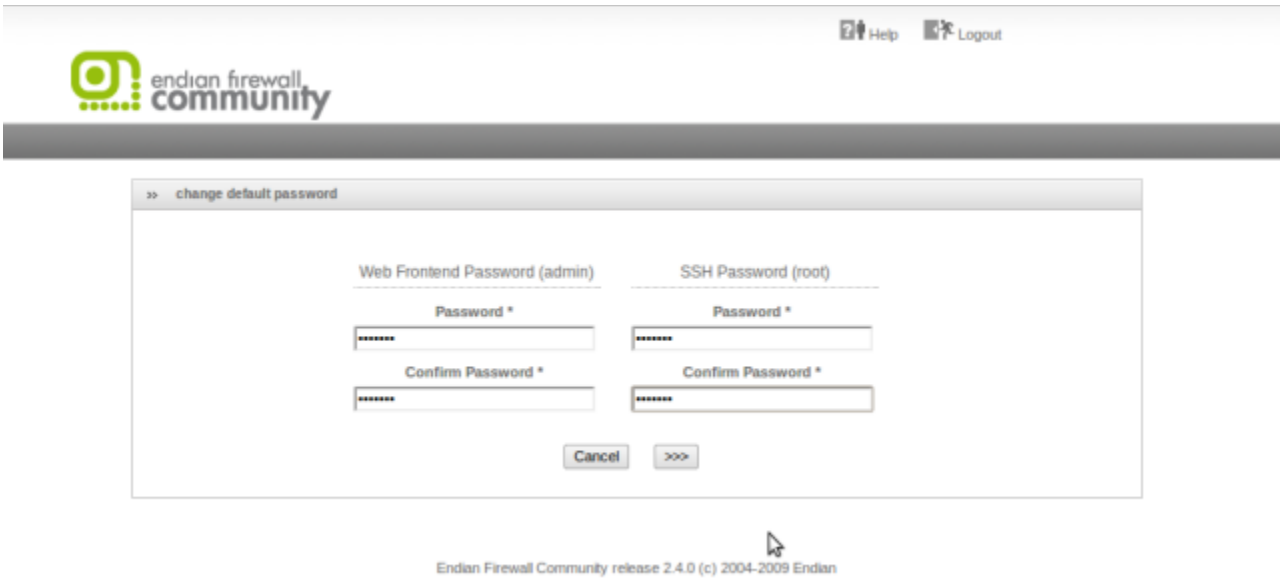

Ilustración 21. Configuración de contraseñas Endian

Ahora vamos a configurar el tipo de conexión que tendrá la interfaz o tarjeta de red que va a estar conectada hacia el router ISP (Internet). En el diagrama de la red podemos ver que estamos utilizando 3 tarjetas de red, la primera está conectada a nuestra LAN (VERDE) y fue la que configuramos antes (recordemos que la configuramos en la instalación de Endian), la segunda es la que vamos a configurar en

este momento (ROJA) y por último configuraremos la de la DMZ (NARANJA). Para comenzar seleccionamos la opción que más se ajuste a nuestras necesidades para configurar la interfaz ROJA. En este caso escogemos Ethernet Estatico, al seleccionar esta opción debemos contar con un una IP fija del segmento del enlace que provee internet.

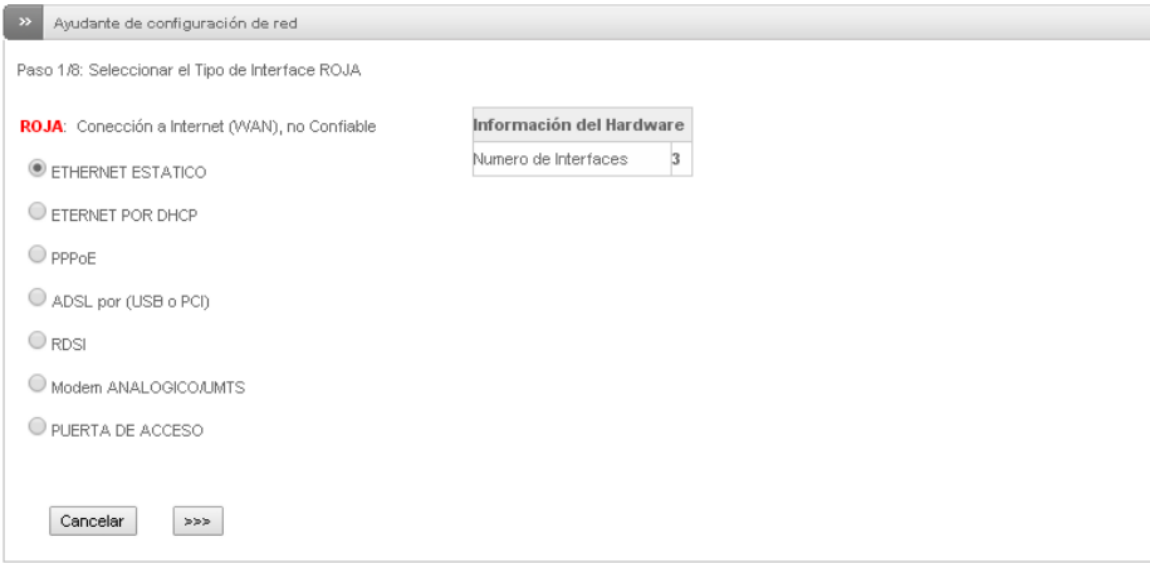

Ilustración 22. Tipo de conexión de la interfaz

Como contamos con una tarjeta de red para la DMZ, entonces seleccionamos la opción NARANJA y continuamos.

Ilustración 23. Tarjetas de red

En esta pantalla tenemos la opción de cambiar la dirección IP de la interfaz (VERDE), la dirección IP de la interfaz (NARANJA), asignar el direccionamiento a una interfaz de red específica. Asignarle el nombre al servidor y el dominio al cual pertenece.

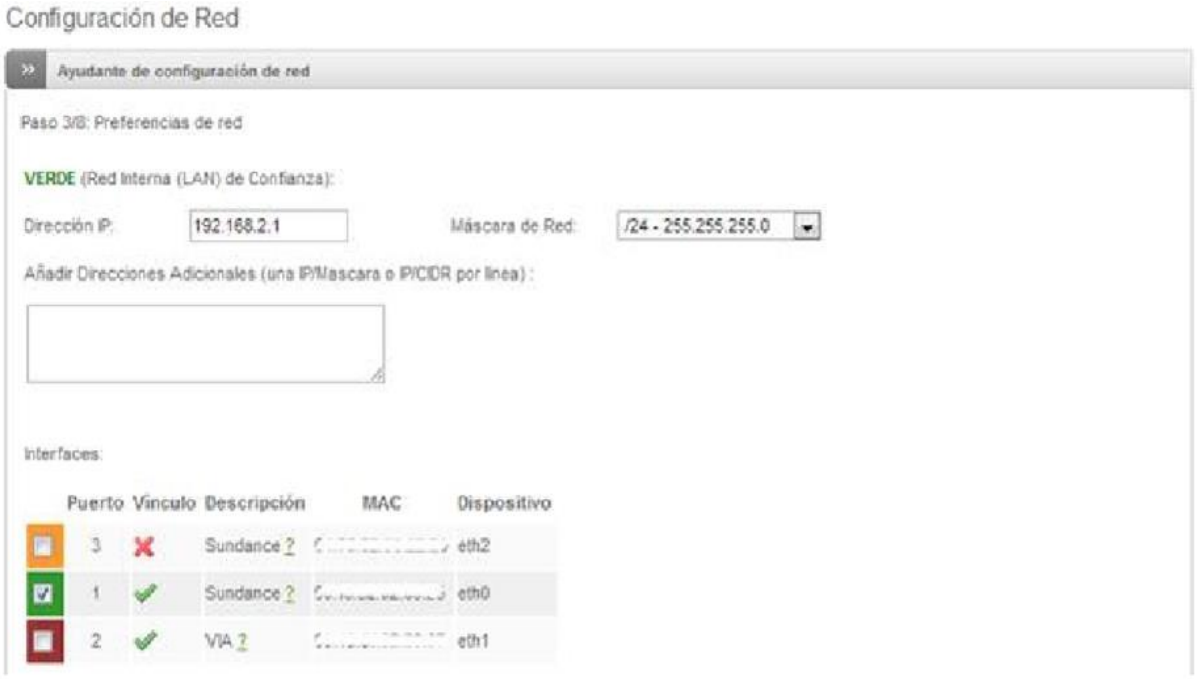

Ilustración 24. Interfaz de red 1

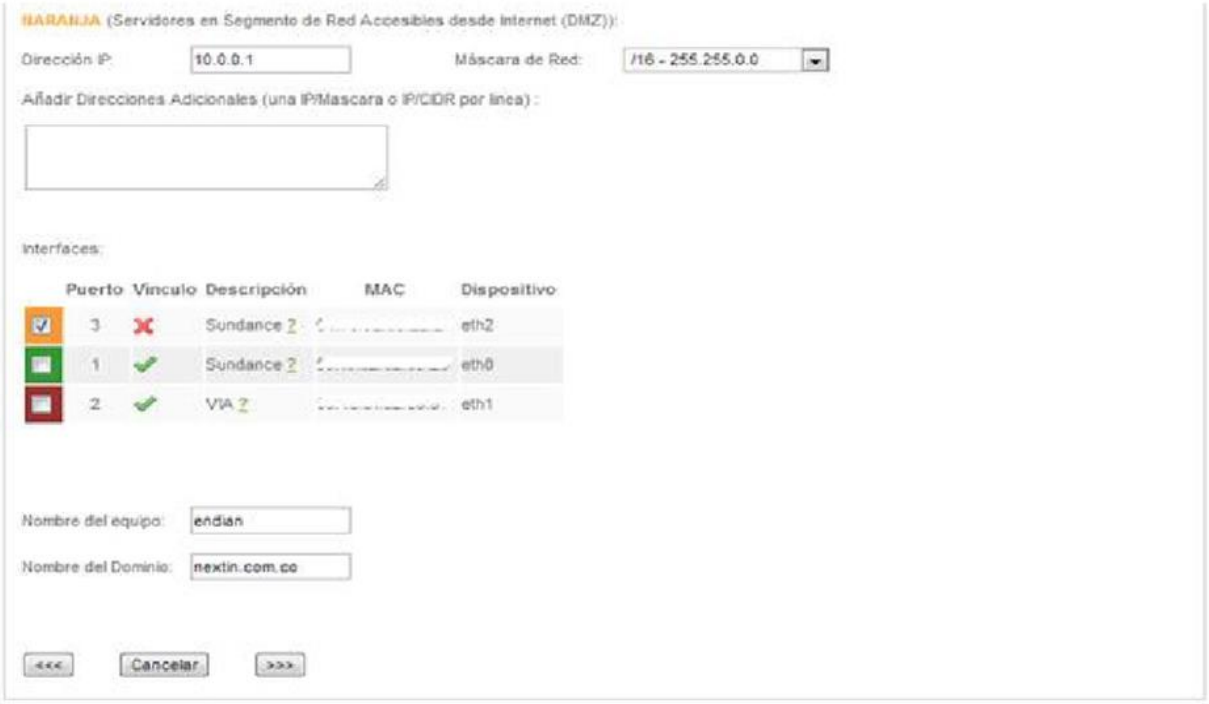

Ilustración 25. Interfaz de red 2

A continuación observamos una imagen similar a la anterior pero en este caso solo vamos a configurar la interfaz de red (ROJA) la cual conecta a internet, lo que hacemos es ingresar la dirección IP del segmento de red del enlace que nos proveerá internet.

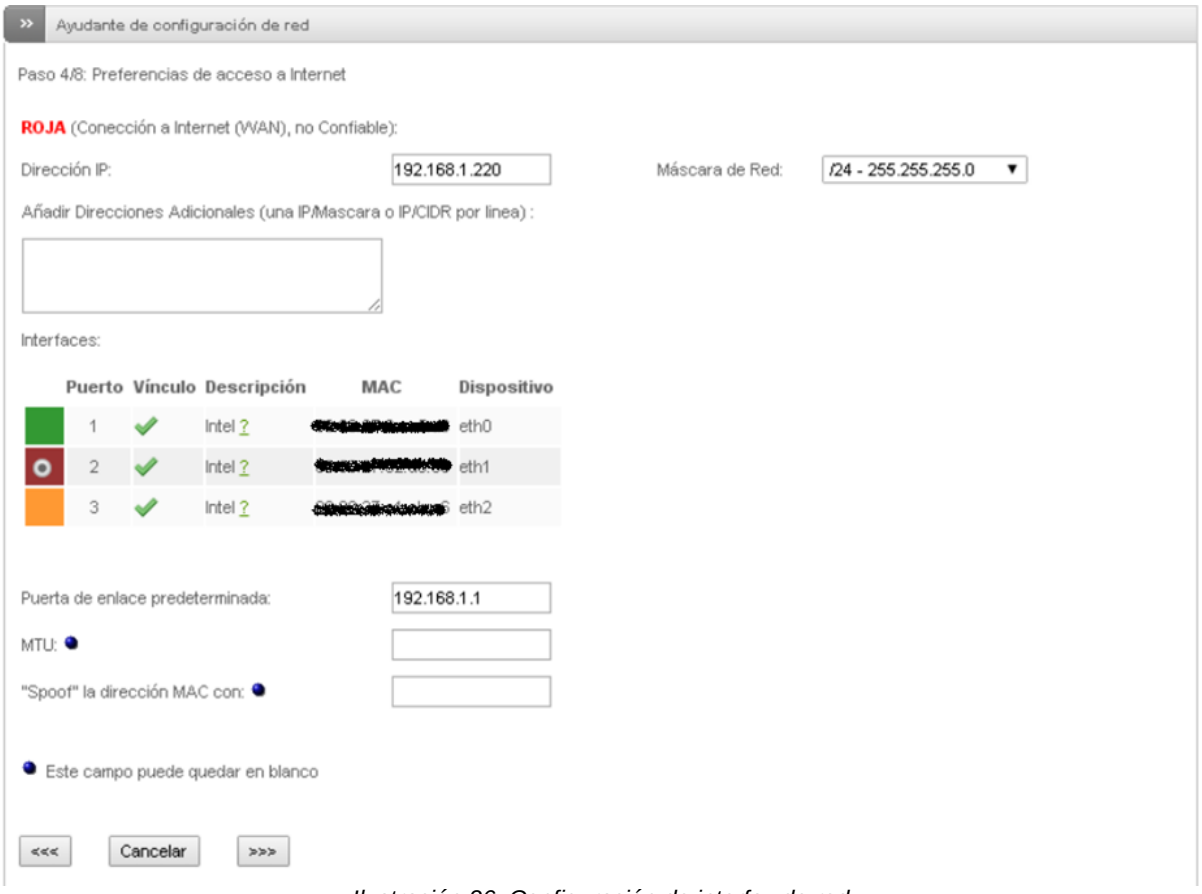

Ilustración 26. Configuración de interfaz de red

Ahora escribimos las direcciones IP de nuestros servidores DNS en el caso de que contemos con ellos de los contrario debemos colocar unos externos.

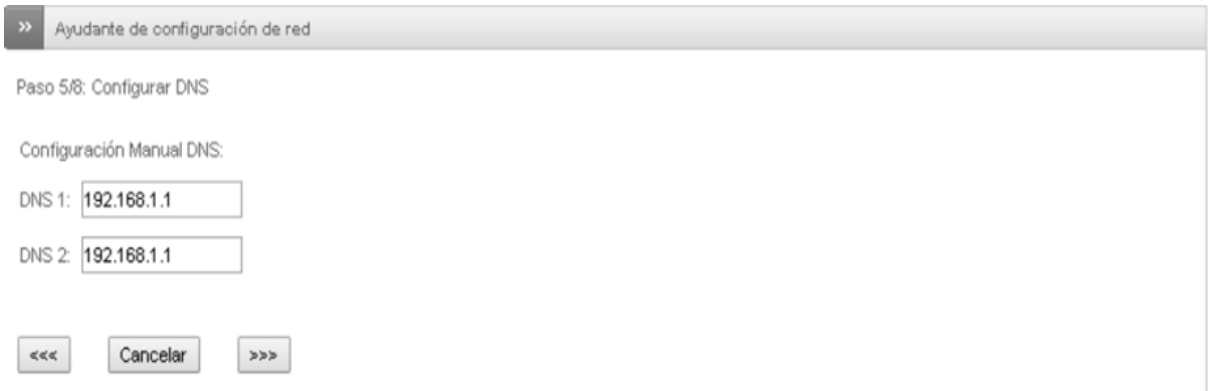

Ilustración 27. Configuración IP y DNS

Después Endian nos pedirá alguna información acerca del administrador, con el fin, de enviar por correo alarmas y restablecer contraseñas

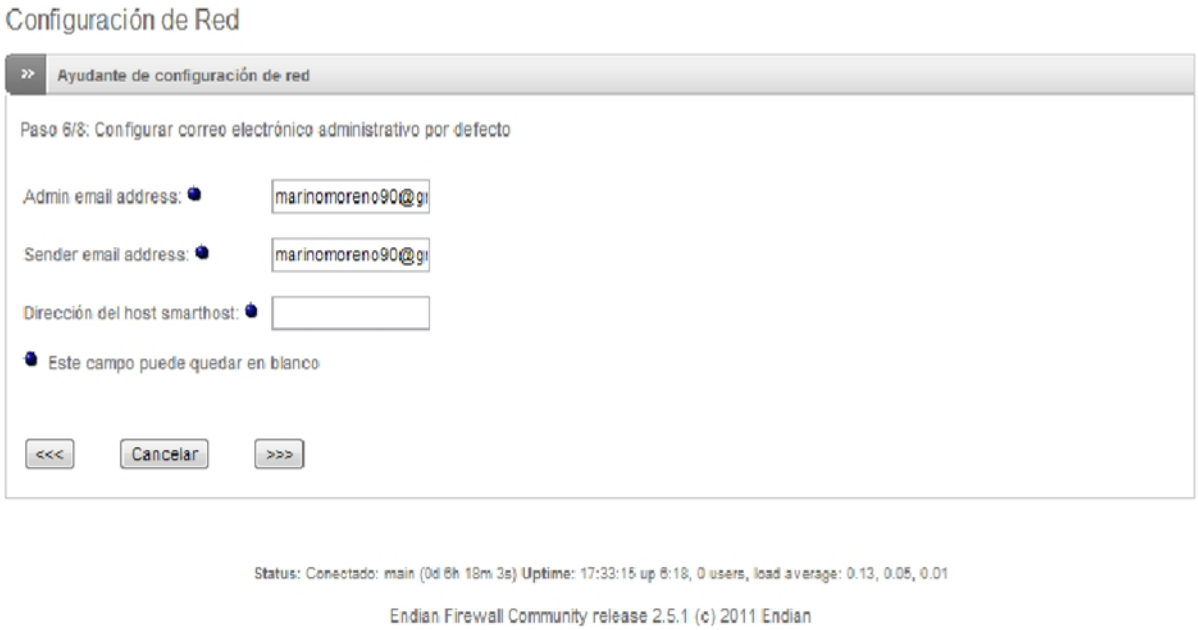

Ilustración 28.Configuración de administrador

Ya en este paso Endian va a aplicar y grabar los cambios y/o configuraciones previamente hechas para esto hacemos clic en OK

Ilustración 29. Guardar las configuraciones

Después de haber aplicado todas las configuración previamente hecha, nuestro servidor se reiniciara automáticamente esto tarda unos minutos.

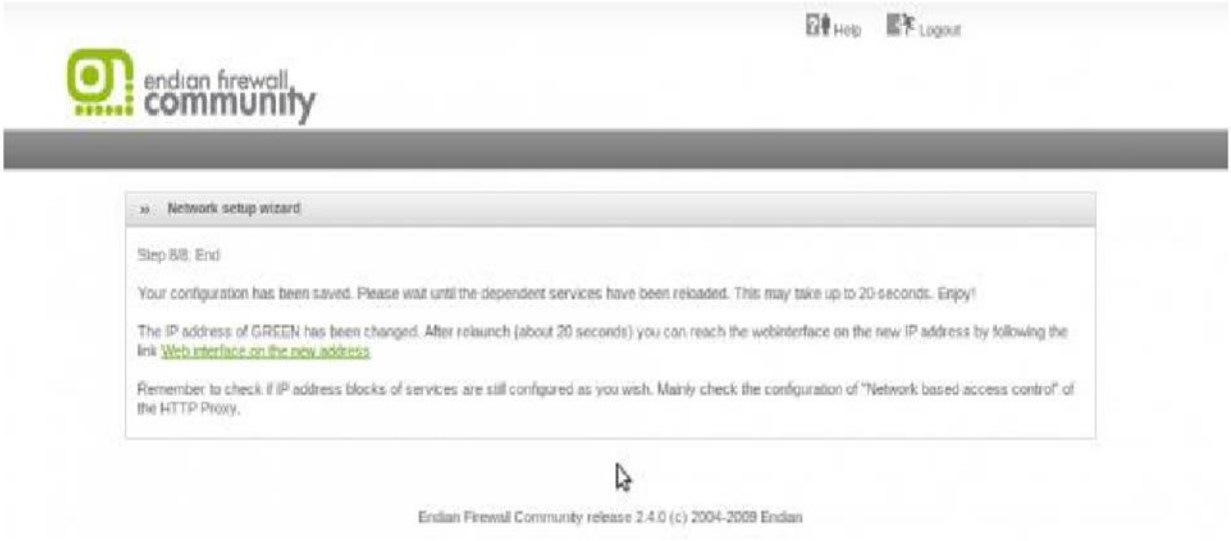

Ilustración 30. Reinicio del sistema

Ya reiniciado nuestro servidor volvemos a entrar la dirección IP de nuestro servidor vía web y cómo podemos ver en la pantalla nos está pidiendo una autenticación, el usuario es admin y la contraseña que nosotros escogimos para este usuario.

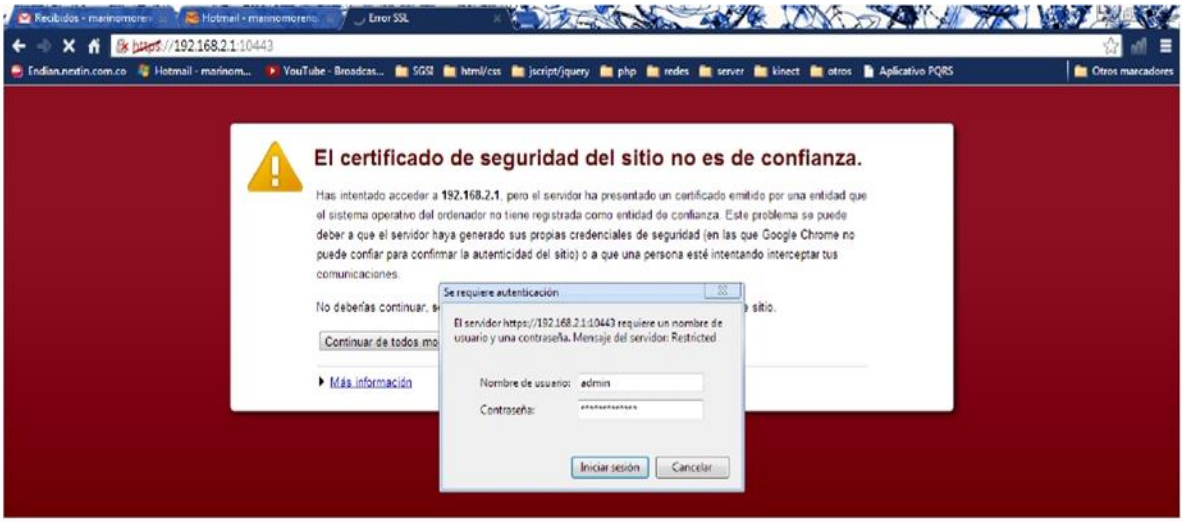

Ilustración 31. Login endian

Podemos ver que ingresamos a la consola de administración de Endian, recordemos que podemos configurar todos los aspectos que están nombrados en las características mencionadas anteriormente.

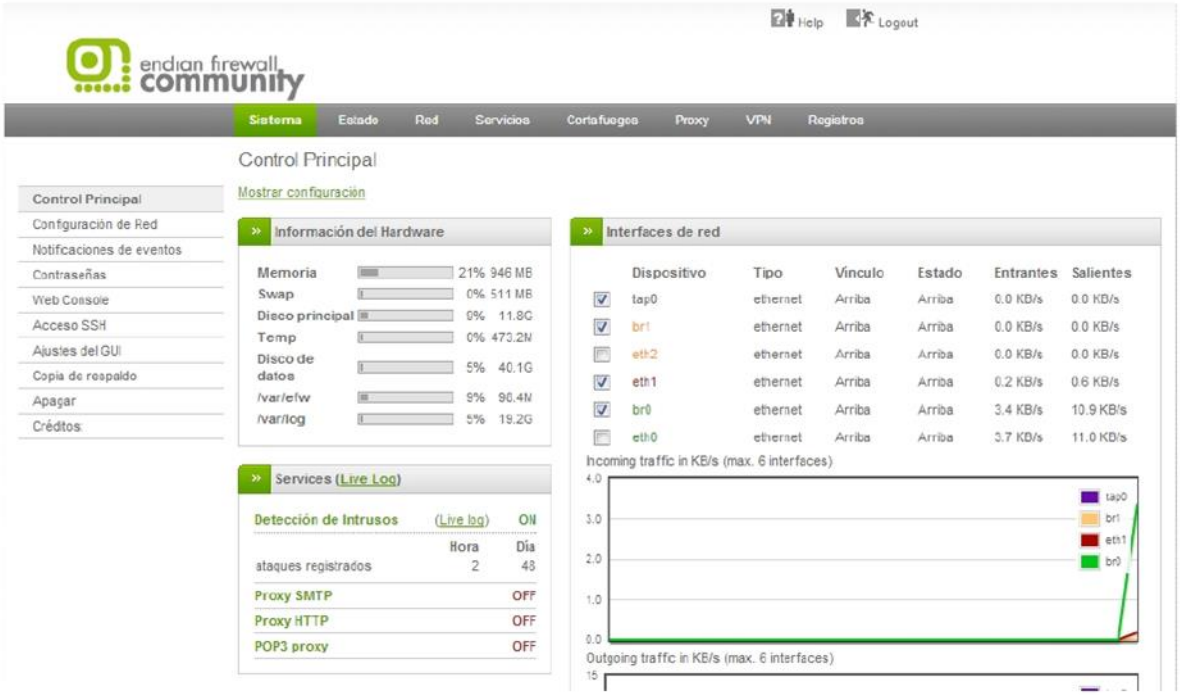

Ilustración 32. Consola de administración de Endian

Ahora vamos a hacer unas pruebas desde un pc conectado en la LAN, por defecto en el firewall Endian está permitido todo el tráfico, verificamos que esto sea correcto, entonces navegamos hacia www.google.com.

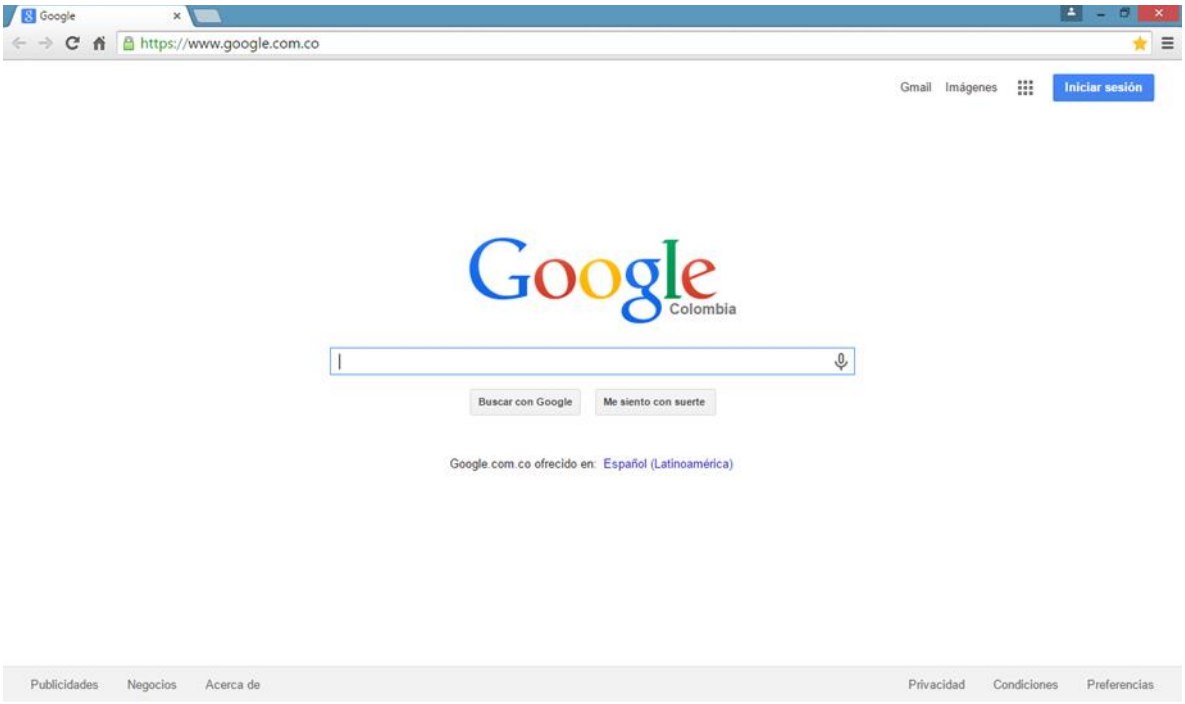

Ilustración 33. Verificación de funcionamiento de Endian

6.2.1 Configuración firewall Endian

Para comenzar a configurar el firewall tenemos que tener identificadas las zonas a las cuales vamos a aplicarles las políticas de acceso con sus respectivas direcciones IP. En nuestro caso contamos con 3 zonas:

- LAN (**Zona Verde**), dirección IP: 192.168.2.0/24
- Internet (**Zona Roja**), dirección IP: 192.168.1.0/24
- DMZ (**Zona Naranja**), dirección IP: 10.0.0.0/16

Después de haber accedido al panel de administración del Endian, nos dirigimos a la opción cortafuegos en el menú principal.

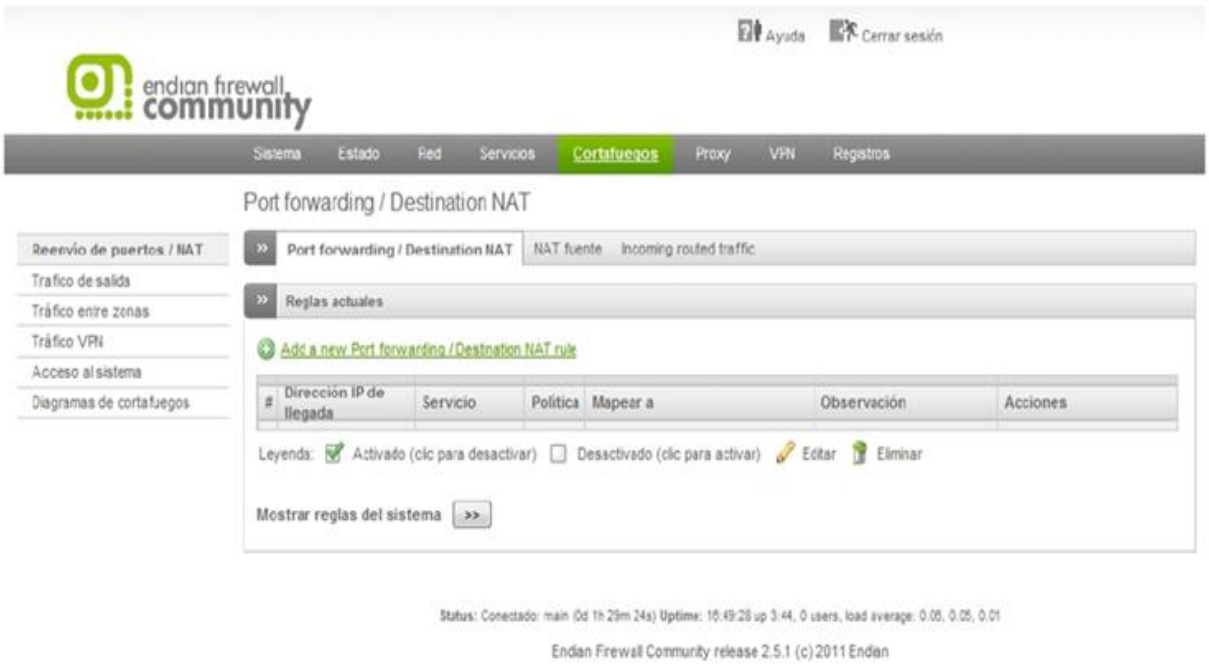

Ilustración 34. Opción cortafuegos

Seleccionamos la pestaña NAT fuente y hacemos click en el enlace Anadir una nueva regla de NAT fuente.

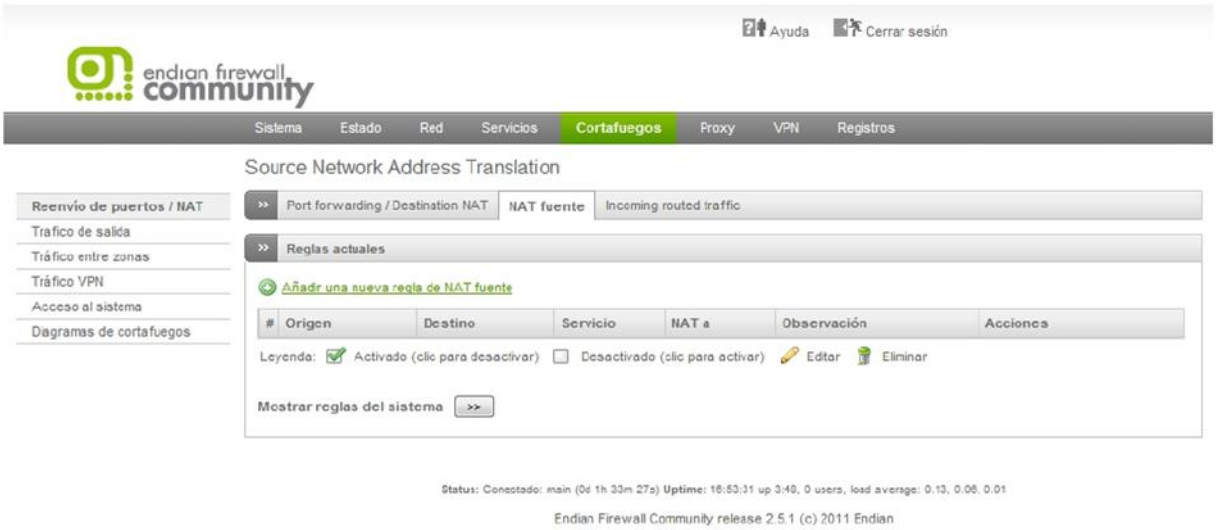

Ilustración 35. Pestaña NAT fuente

A continuación seleccionamos en tipo RedIP tanto para el origen como para el destino.

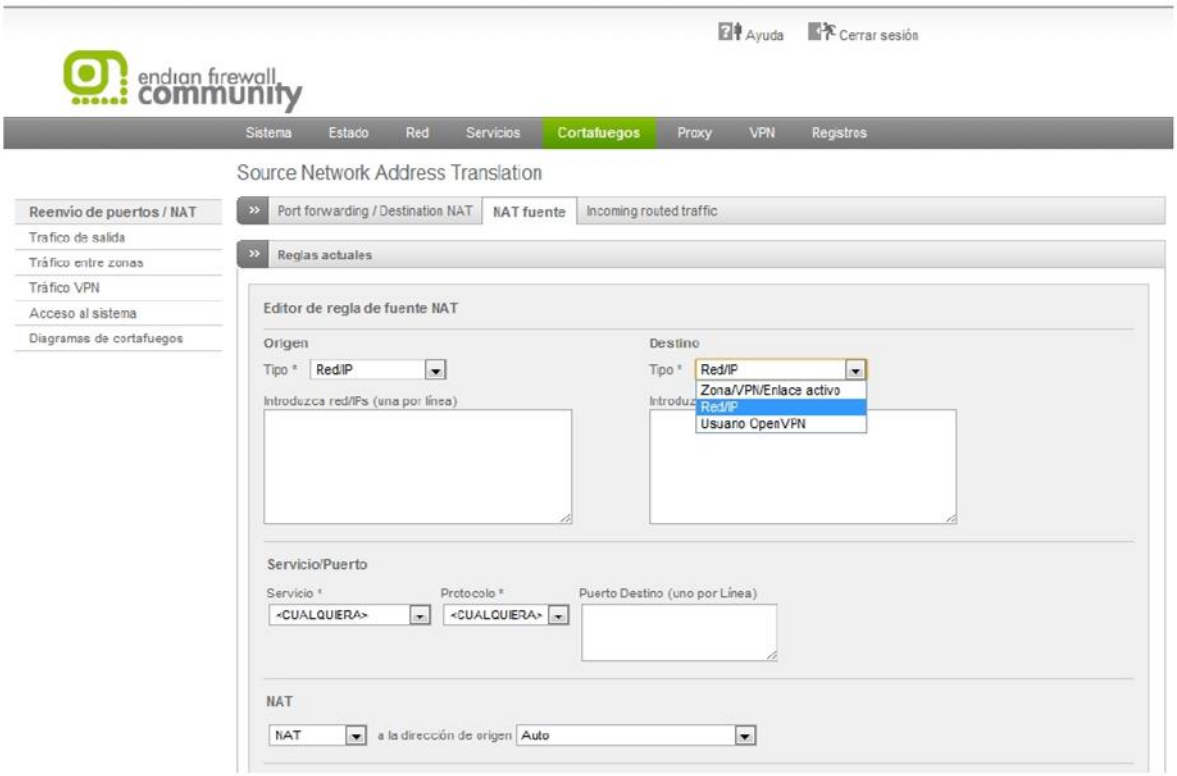

Ilustración 36. Tipo redIP

Introducimos en el origen la dirección de red de la LAN 192.168.2.0 con su máscara /24 a continuación en el destino escogemos la opción Tipo

Zona/VPN/Enlace activo y seleccionamos Enlace activo Enlace principal [ROJA]. En la sección NAT a la dirección seleccionamos Enlace activo Enlace Principal.

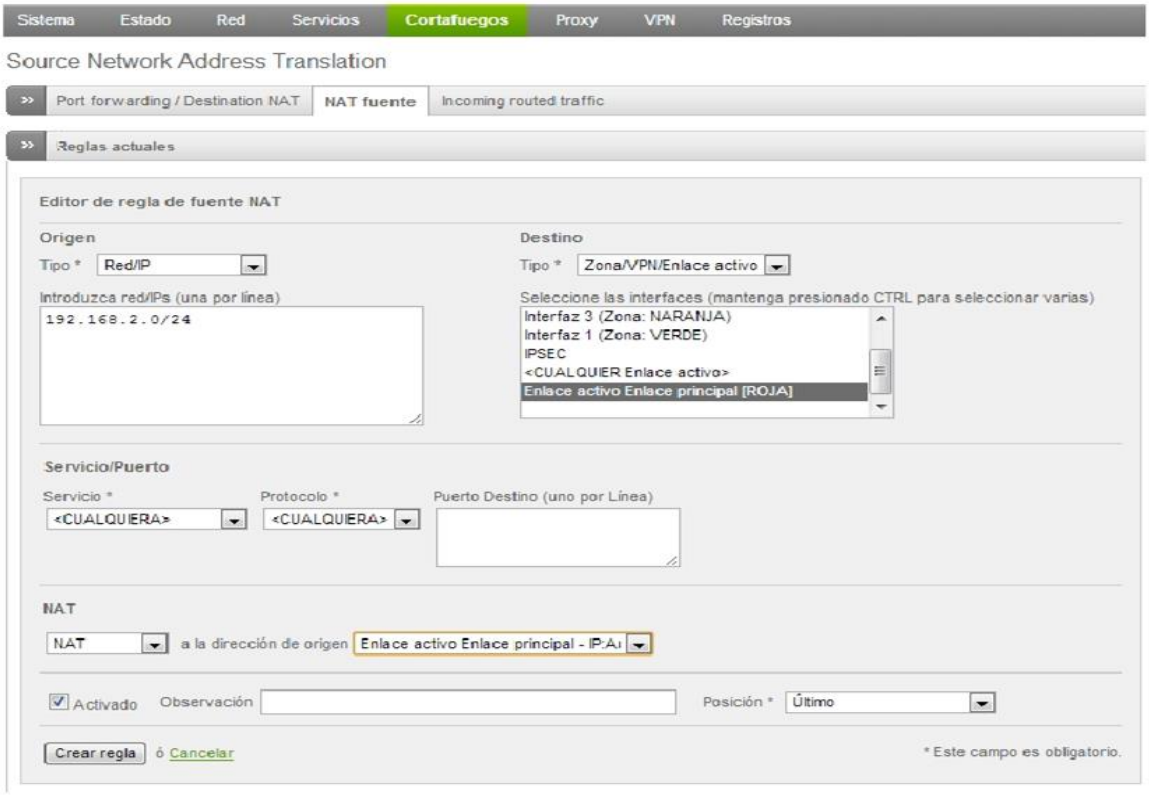

Ilustración 37.Añadir regla NAT LAN-Internet

Hacemos click en el botón crear regla y luego en el botón aplicar.

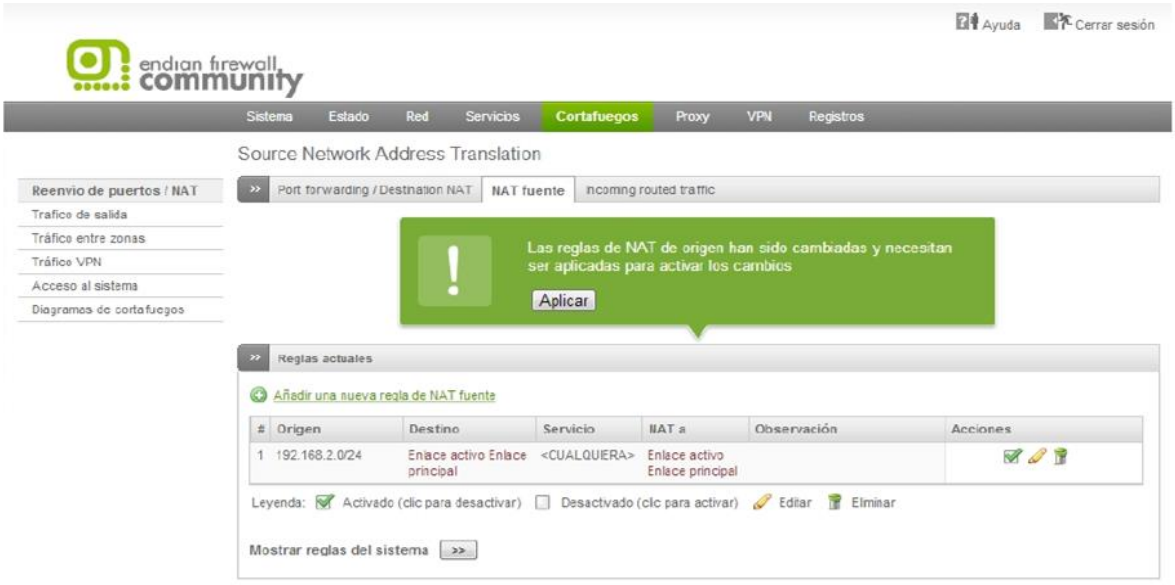

Ilustración 38. Crear regla NAT LAN-Internet

Aplicamos la regla NAT LAN-Internet.

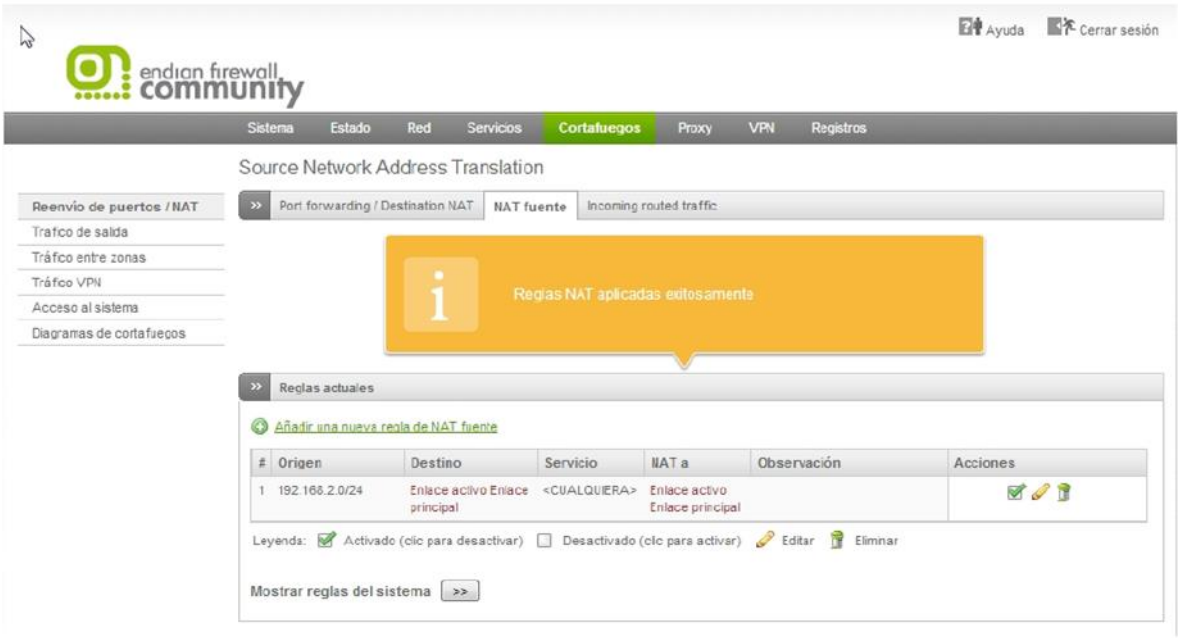

Ilustración 39. Aplicar regla NAT LAN-Internet

Añadimos otra regla donde el origen va a ser la dirección de red de la zona DMZ cuya IP es 10.0.0.0 con mascara de red /16 y el destino sigue siendo el enlace activo o Enlace principal [ROJA].

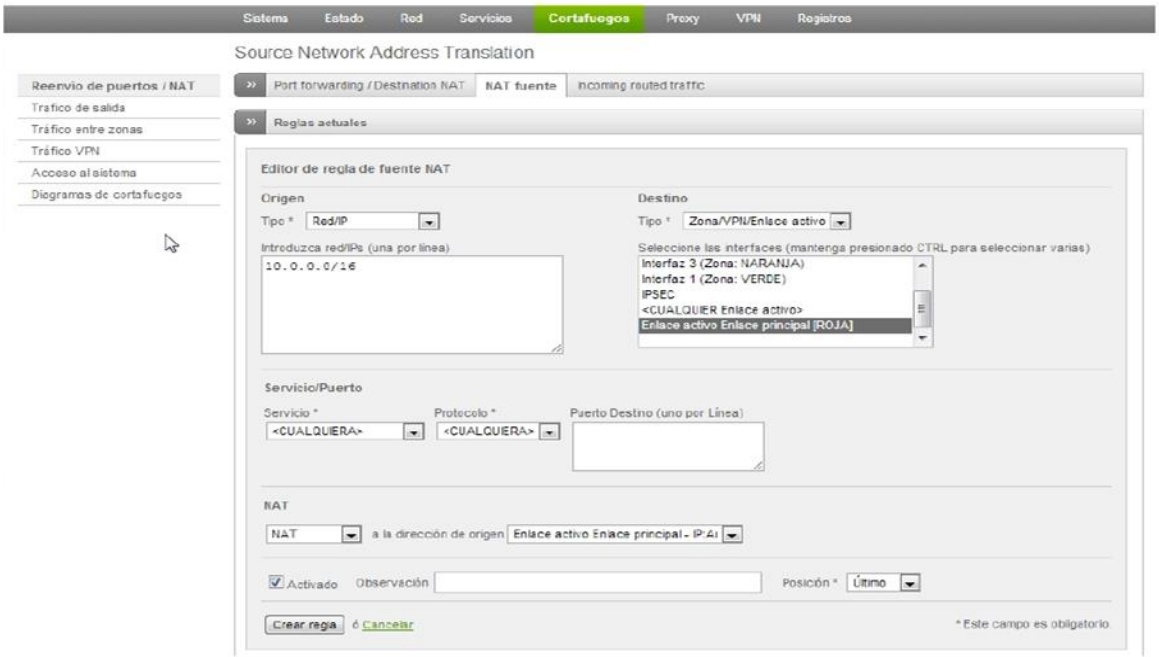

Ilustración 40. Añadir regla NAT DMZ-Internet

Creamos y aplicamos la regla NAT DMZ-Internet

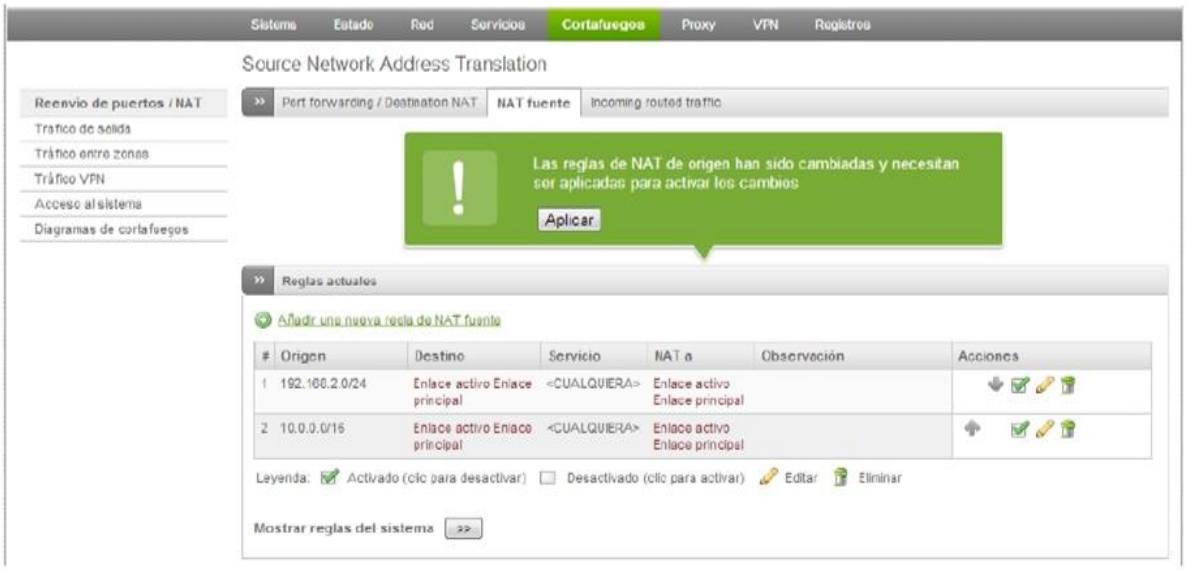

Ilustración 41. Aplicar regla NAT DMZ-Internet

Ahora creamos una nueva regla donde se va a denegar el tráfico de la zona roja hacia la zona verde para esto seleccionamos en el origen la opción <ROJA>

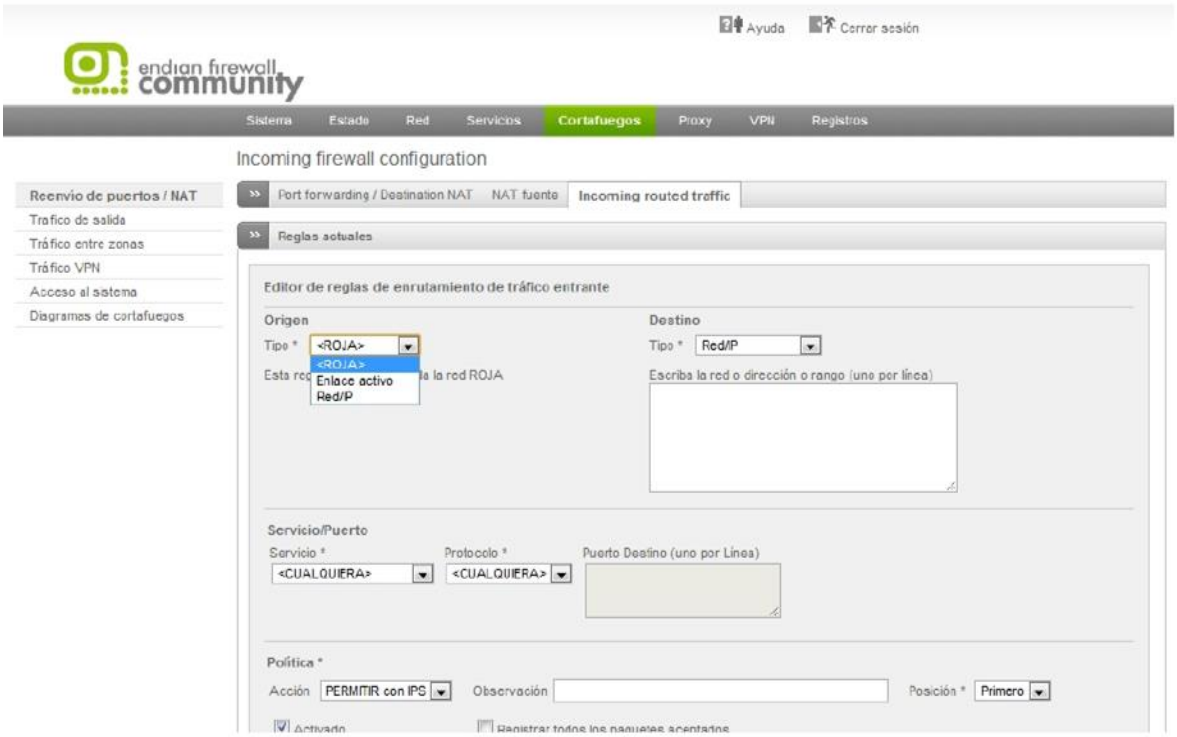

Ilustración 42. Origen Tipo Roja

En el destino seleccionamos la opción zonas y a continuación seleccionaremos la verde.

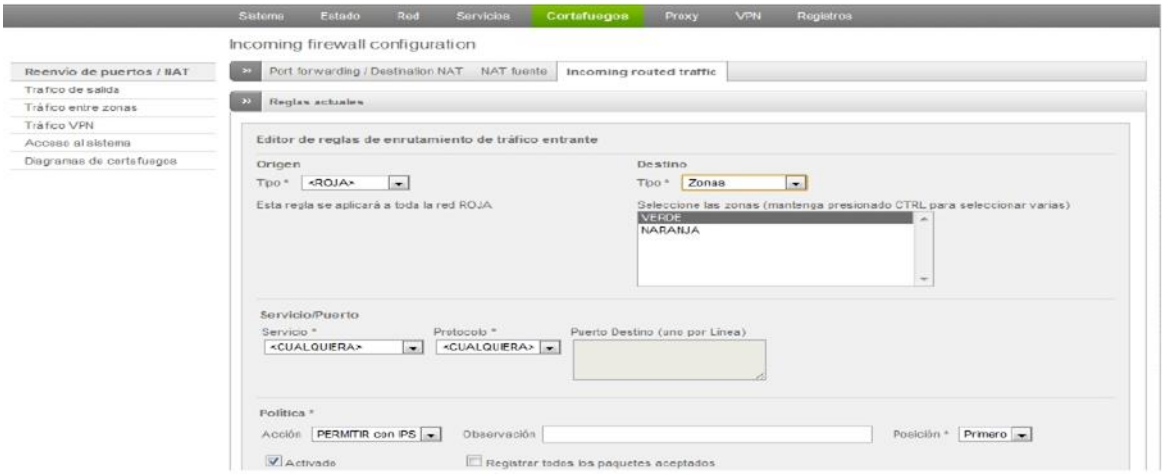

Ilustración 43. Destino Zona Verde

En política la acción que seleccionamos es Denegar.

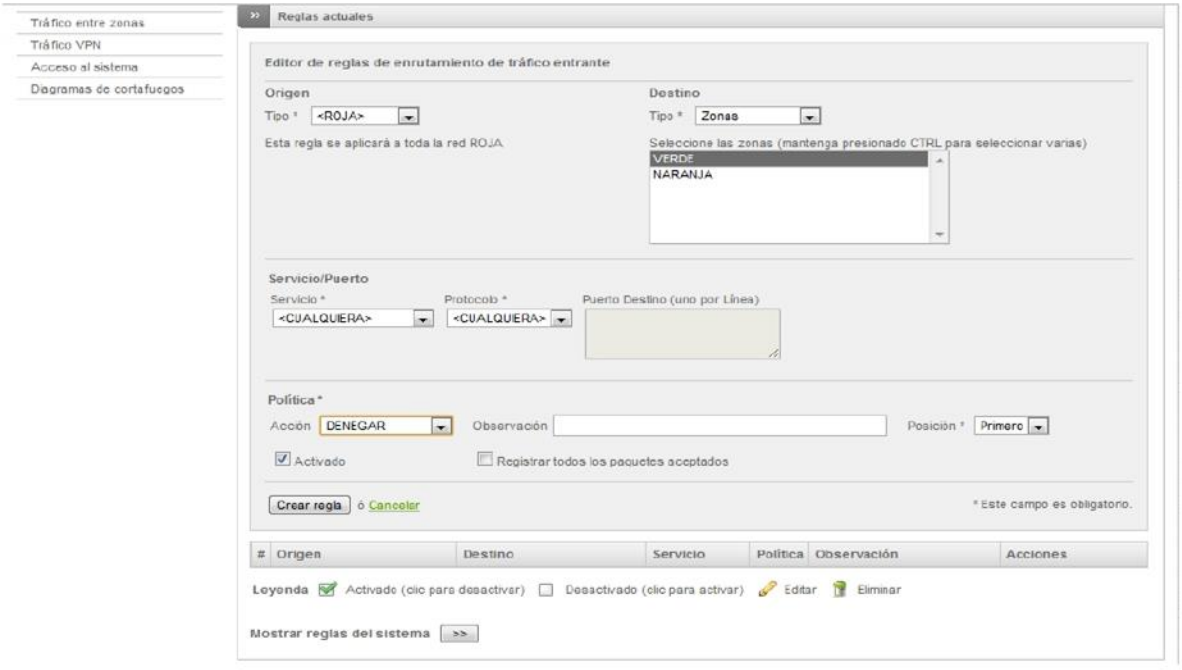

Ilustración 44. Política acción denegar

Creamos y aplicamos la regla.

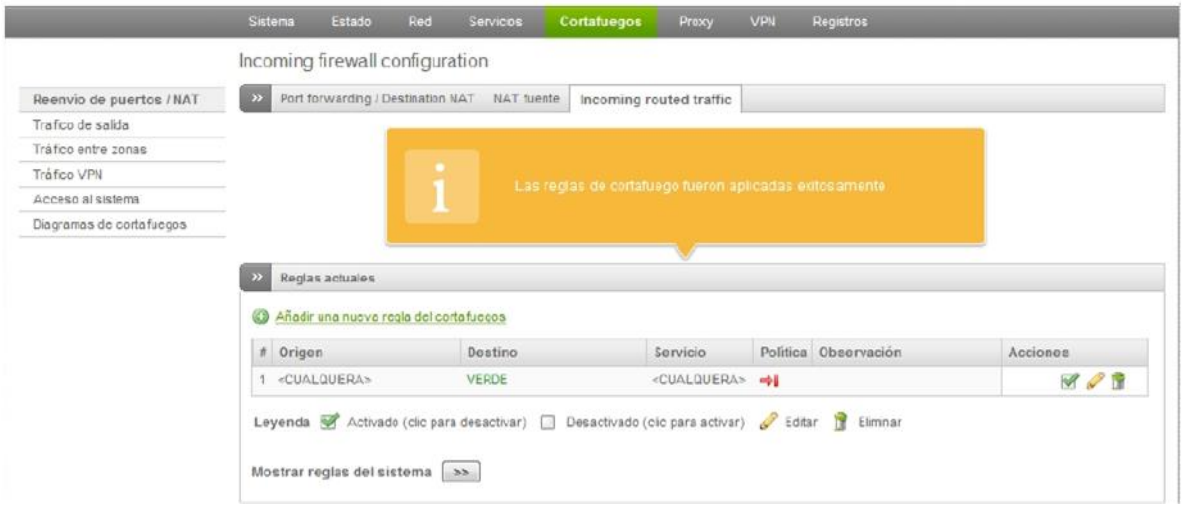

Ilustración 45. Aplicar regla denegar roja-verde

Ahora lo que haremos será crear una política por la cual se tenga acceso de la zona roja a la zona DMZ solo por los puertos que definamos en nuestro caso el puerto 80 (http), el puerto 21 (FTP), el puerto 22 (SSH) y el puerto 5432 (BD Postgres). Para esto seleccionamos la pestaña Port forwarding/ Destination NAT y hacemos click en el enlace add new Port forwarding/ Destination NAT rule.

Ilustración 46. Crear nueva regla port forwarding / destination nat

En la dirección de IP de llegada seleccionamos la interfaz Enlace activo Enlace principal - IP Todos los conocidos.

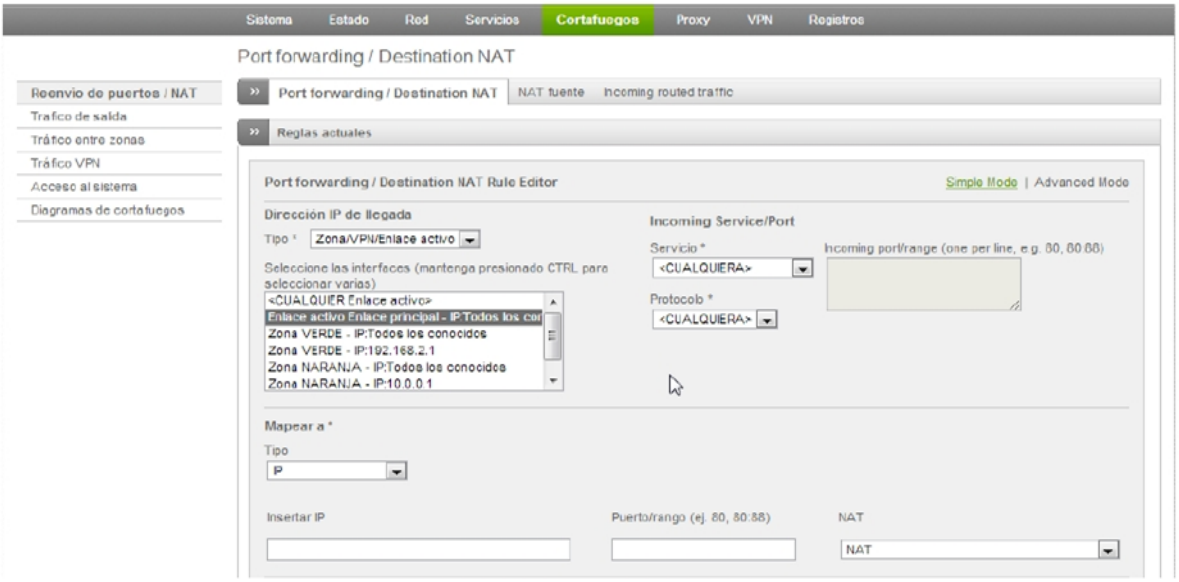

Ilustración 47. Seleccionar enlace activo principal

Seguidamente en incoming service / port seleccionamos el servicio que queremos tener acceso en este caso FTP.

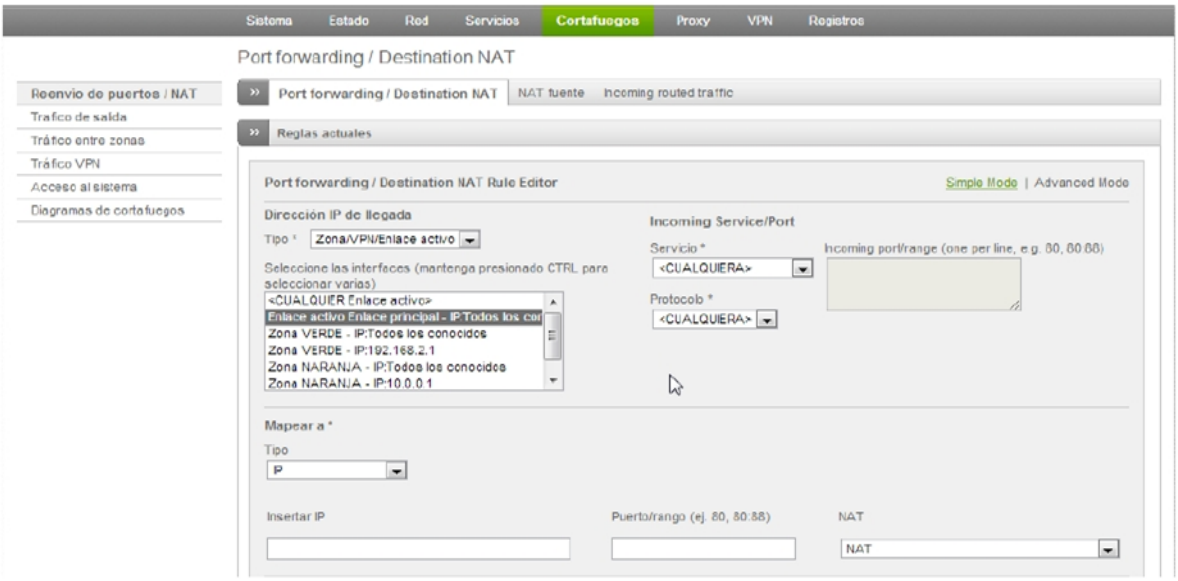

Ilustración 48. Seleccionar servicio FTP

En insertar IP digitamos la dirección IP y el puerto del servidor que aloja el servicio FTP. La cual es 10.0.0.2 y el puerto el 21.

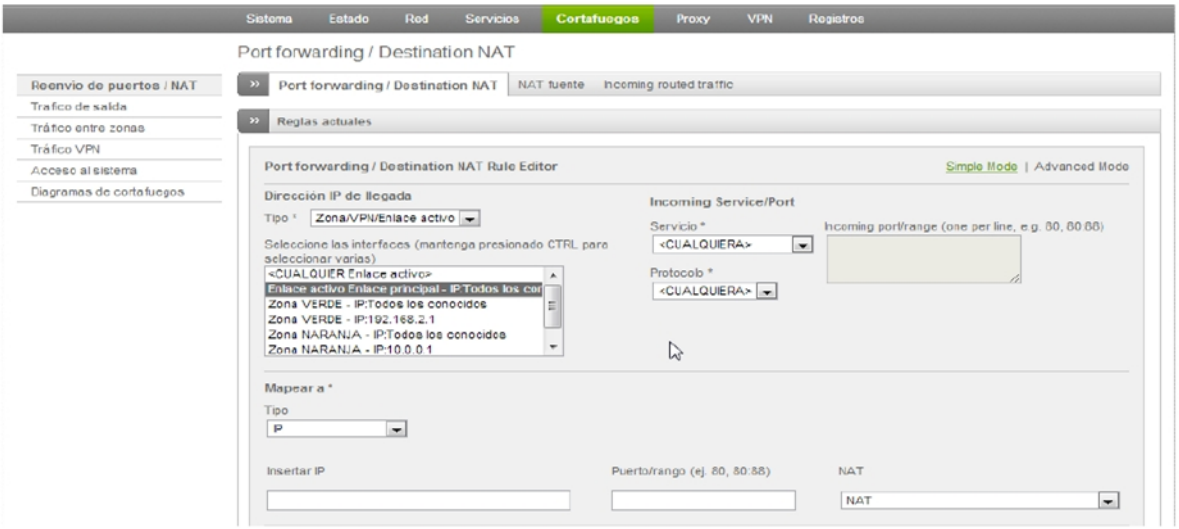

Ilustración 49. Digitación de IP de servidor

Creamos y aplicamos la regla

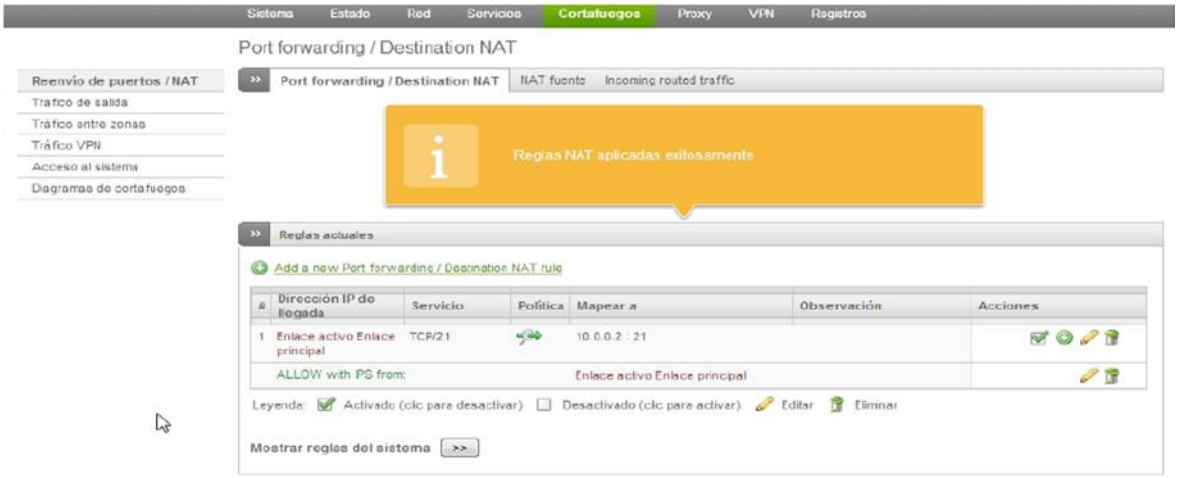

Ilustración 50. Crear y aplicar regla

Creamos una nueva regla para tener acceso desde la zona roja (Internet) a la DMZ por el puerto 80 (http). Para esto seleccionamos el Enlace principal Enlace activo, seguidamente escogemos el servicio http y digitamos la IP y el puerto del servidor que contiene el servicio http. Hacemos lo mismo para los servicios restantes SSH (puerto 22) y BD postgres (puerto 5432) solo que variaremos la escogencia de los puertos según el caso, omitiremos los pantallazos de la configuración.

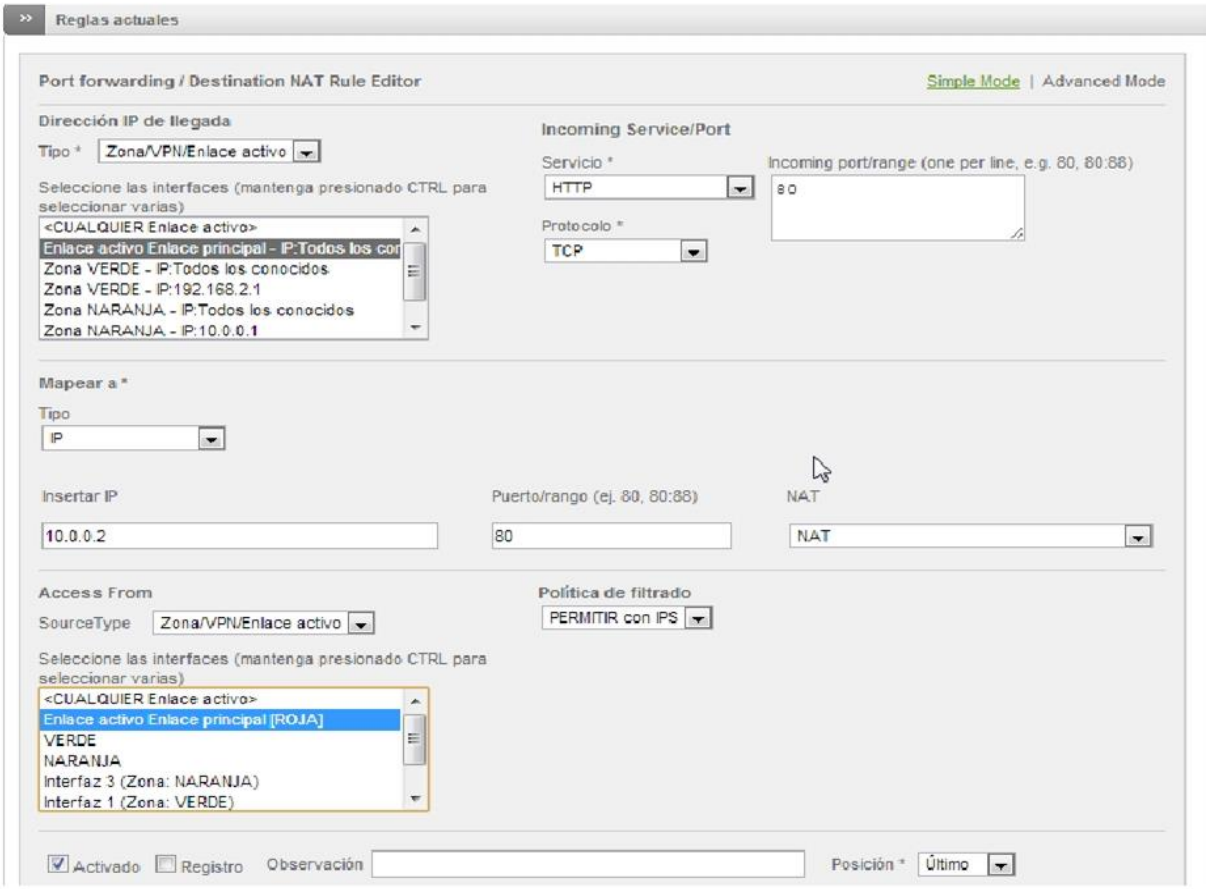

Ilustración 51. Crear regla acceso internet - DMZ puerto 80

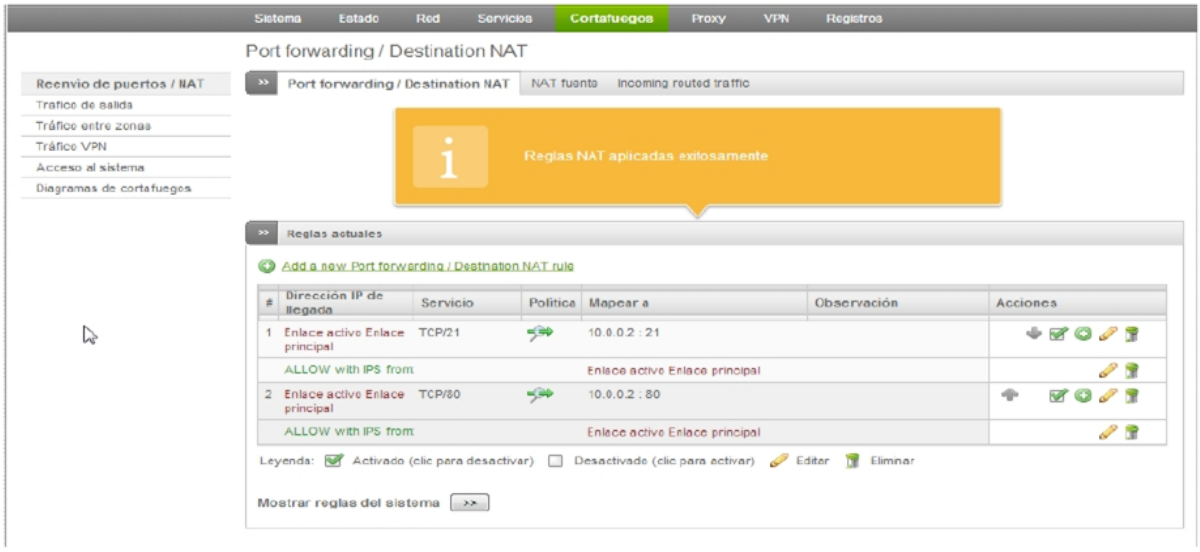

Ilustración 52. Crear y aplicar regla

Ahora lo que vamos a hacer es crear una política donde sea denegado el tráfico de la zona Naranja (DMZ) hacia la zona verde (LAN). Para esto seleccionamos la opción tráfico entre zonas. Por defecto vamos a encontrar unas creadas.

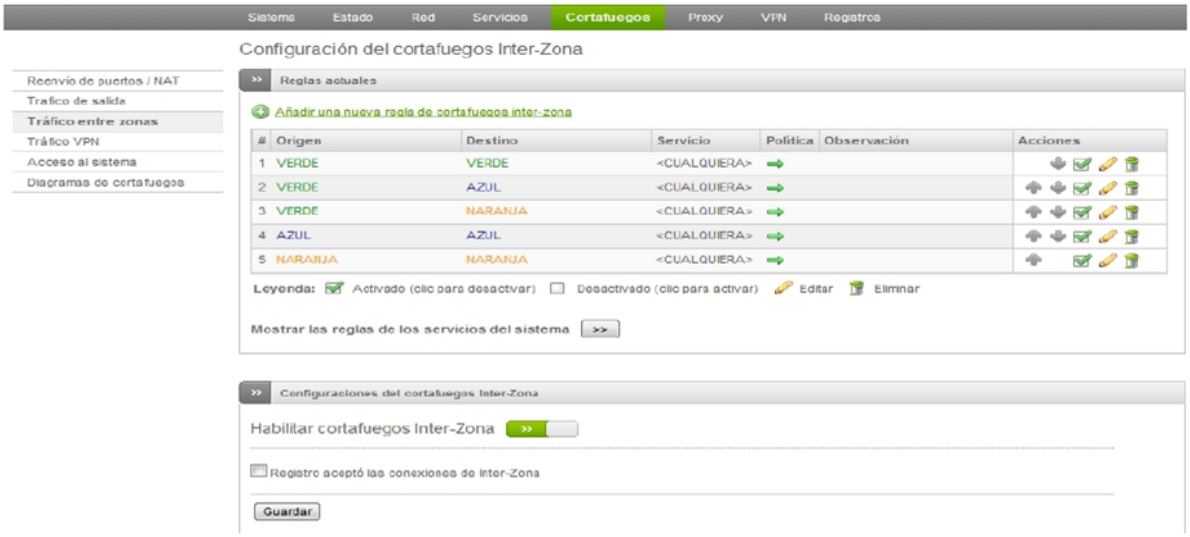

Ilustración 53. Opción tráfico entre zonas

Añadimos una nueva regla de cortafuego inter-zona.

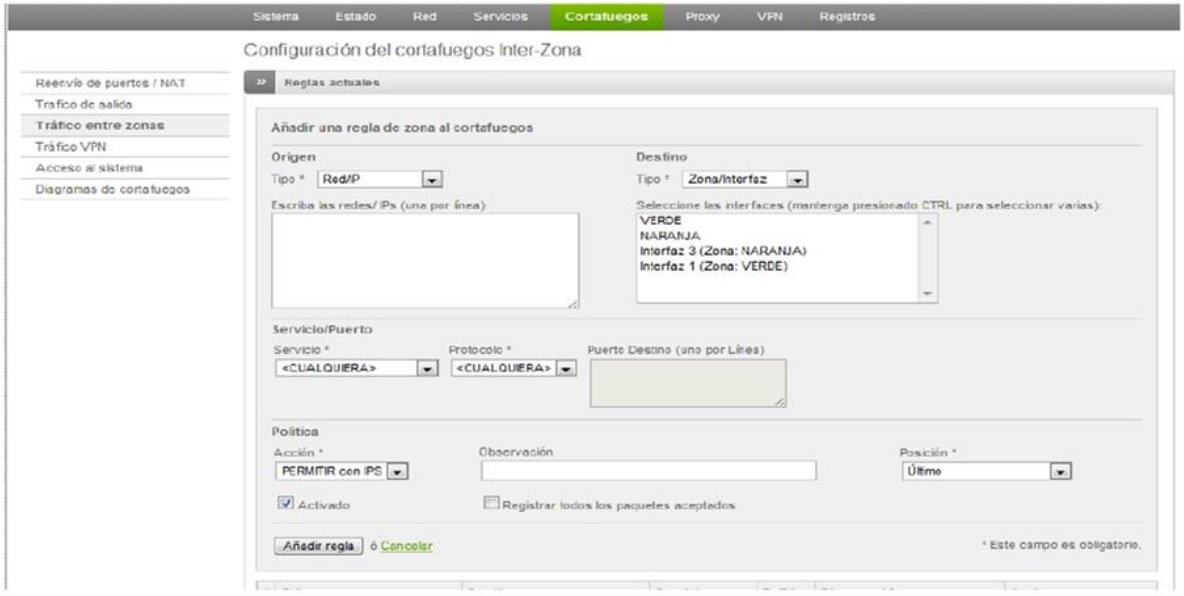

Ilustración 54. Añadir nueva regla de cortafuegos inter-zonas

En origen y destino seleccionamos el tipo Zona/Interfaz

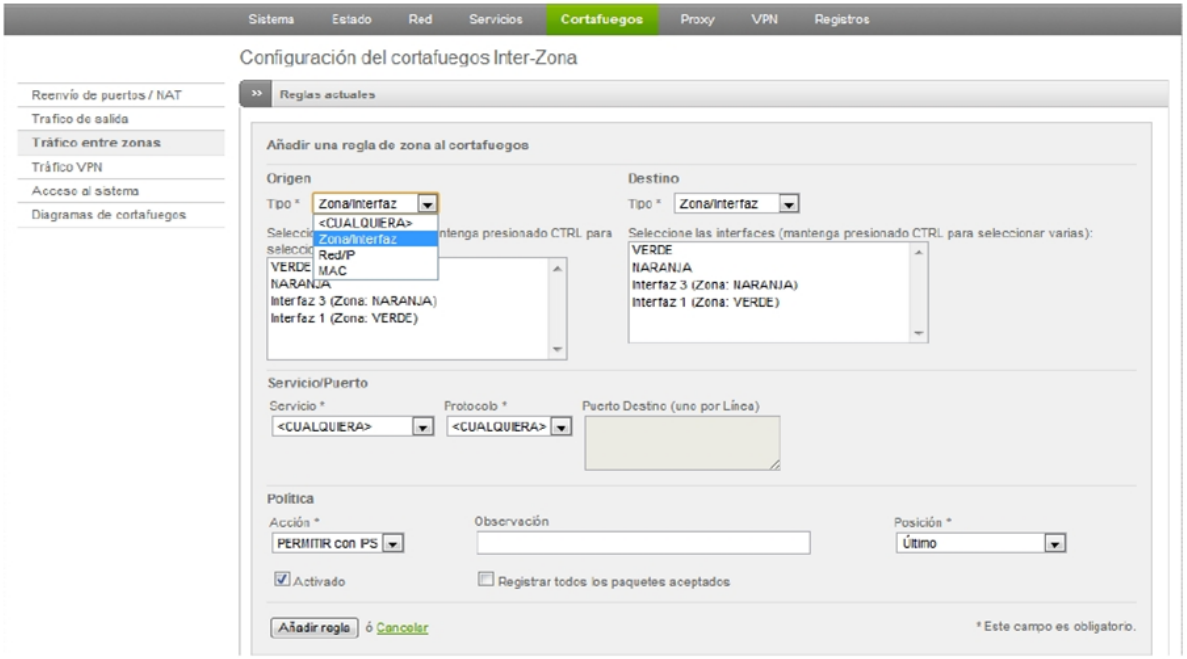

Ilustración 55. Seleccionar origen y destino zona / interfaz

Seleccionamos en el origen la opción Naranja y en el destino la opción Verde.

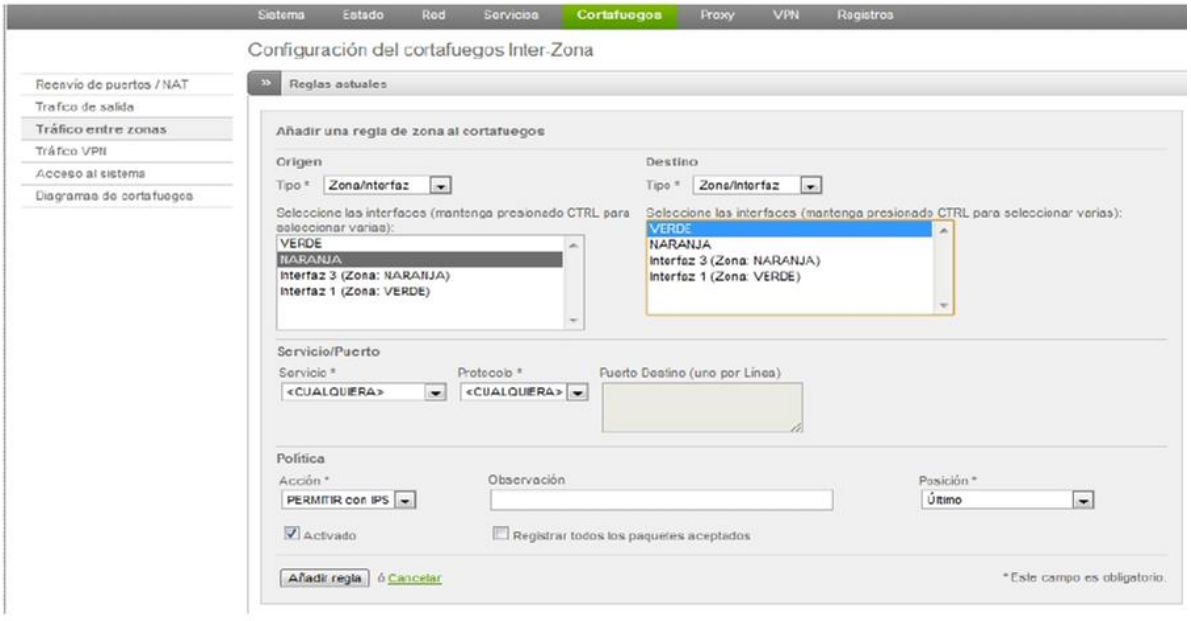

Ilustración 56. Seleccionar origen naranja y destino verde

En política escogemos la acción denegar.

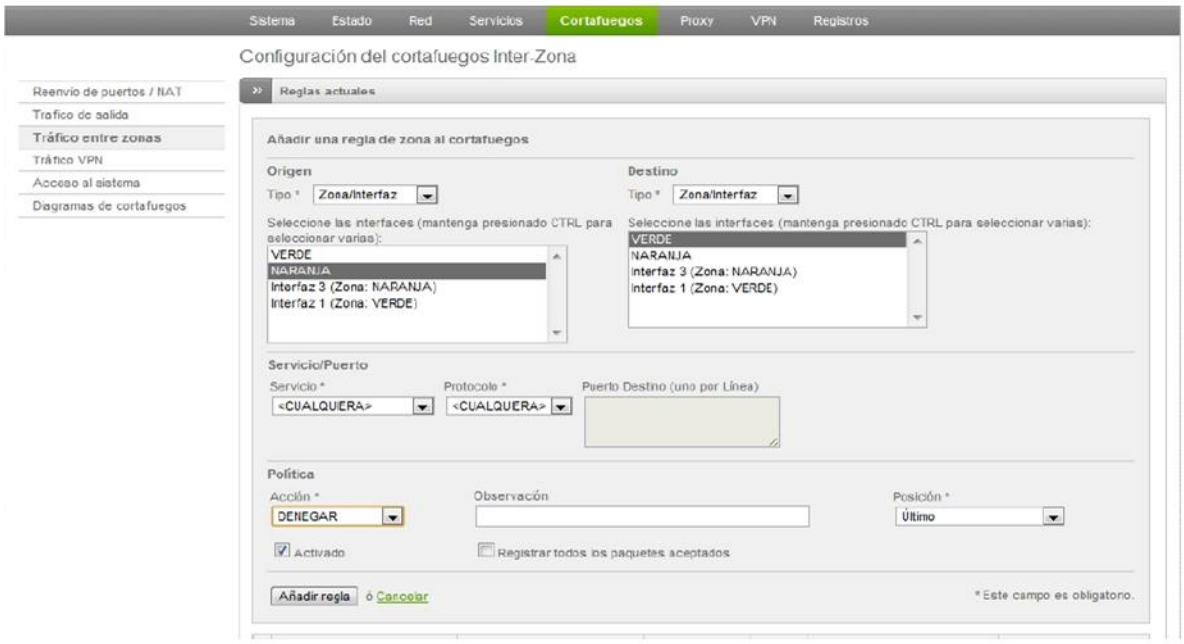

Ilustración 57. Seleccionar la acción denegar

Creamos y aplicamos la regla.

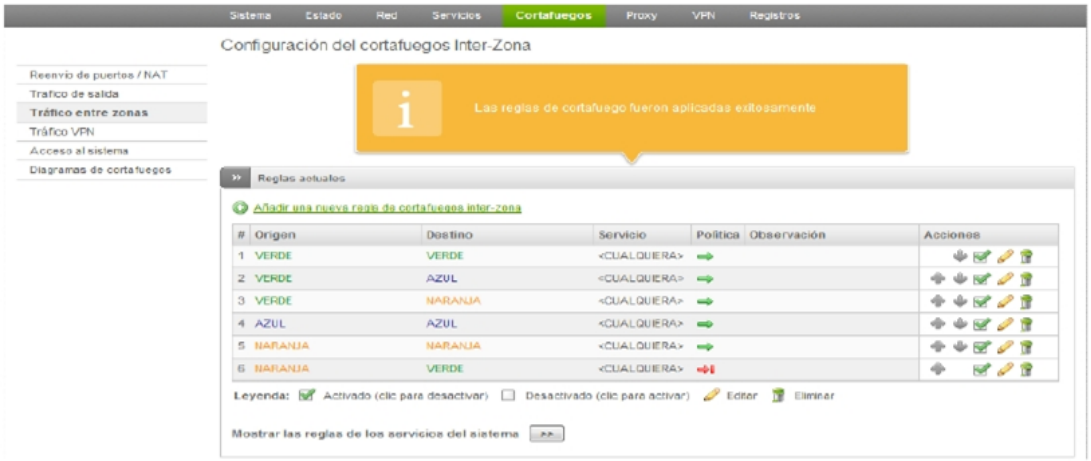

Ilustración 58. Crear y aplicar

Después de realizar las configuraciones del firewall, necesitamos que se pueda acceder desde internet al servicio http alojado en el servidor 10.0.0.2 de la DMZ, para esto seleccionamos en el menú principal Red>Enrutar>Politica de ruteo.

Editamos los campos de Origen 192.168.1.220 y en el destino 10.0.0.2, a continuación seleccionamos en servicio/puerto HTTP y la vía de la ruta escogemos la puerta de enlace estática 10.0.0.1. Por ultimo guardamos y aplicamos la configuración.

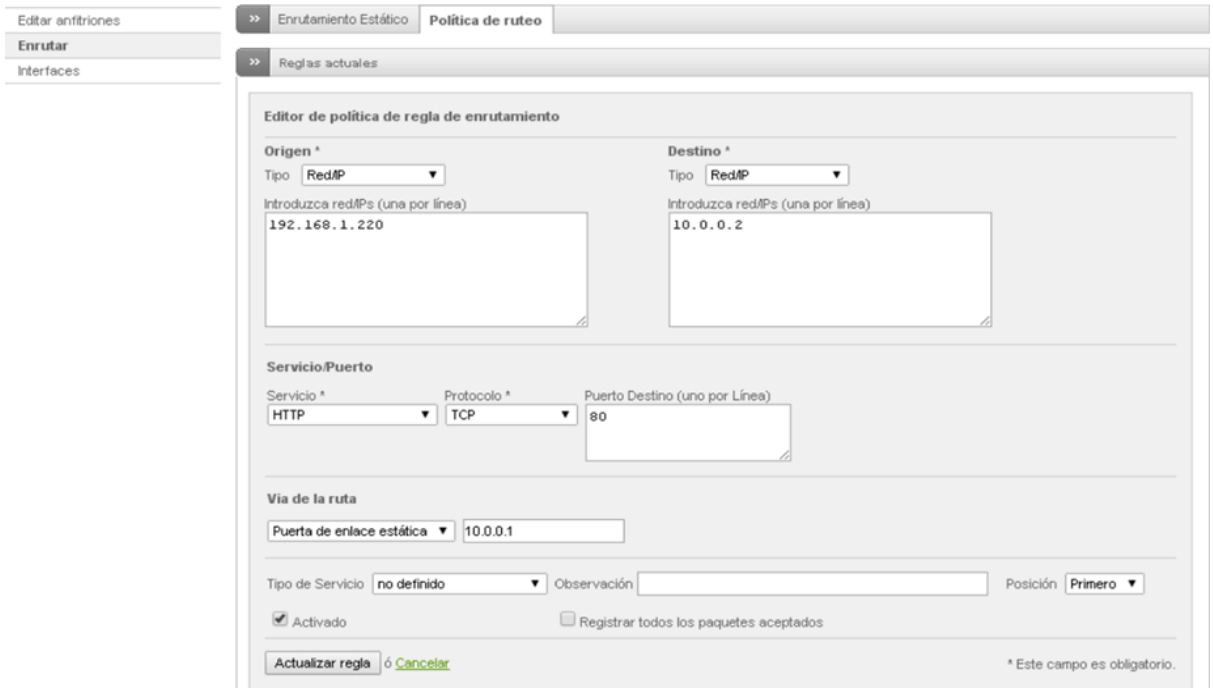

Ilustración 59. Política de ruteo Internet - Server http

6.2.2 Configuración Proxy Web Endian

Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a conexiones Web.

Vamos a implementar una solución de proxy, que contenga autenticación de usuarios, que filtre el contenido, y deniegue o permita el acceso a páginas web. Para esto se crearon grupos de usuario por cada área del hospital, usuarios por cada equipo en el área correspondiente y se definieron tres niveles de filtrado por sensibilidad de contenido web permitido. Los niveles se denotaron como filtrado alto, filtrado medio y filtrado bajo.

Después de autenticarnos en el panel web de administración de Endian, seleccionamos la opción Proxy en el menú principal.

Ilustración 60. Opción proxy Endian

Habilitamos el proxy HTTP

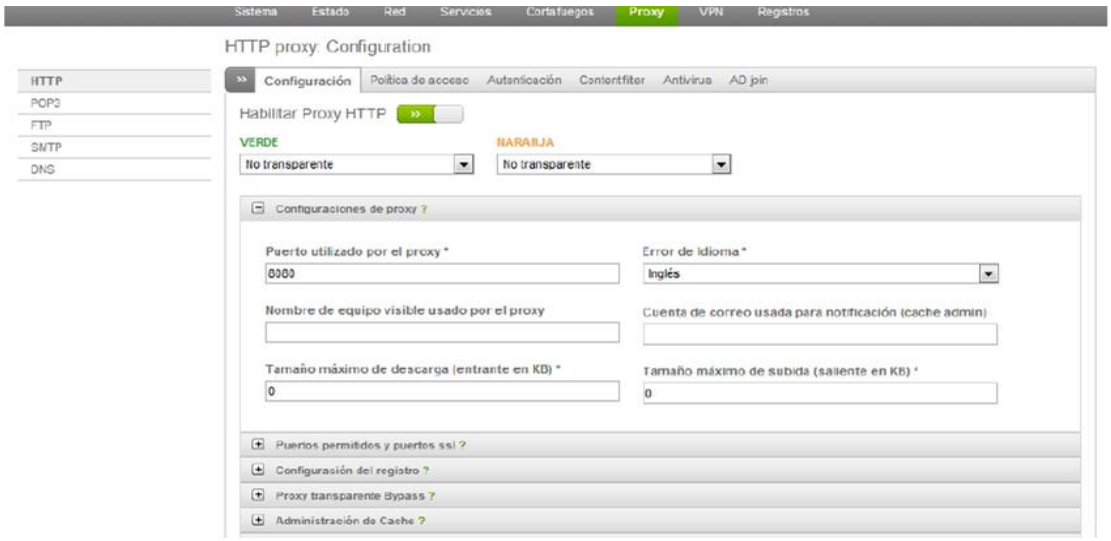

Ilustración 61. Habilitar proxy HTTP

En la opción del menú acordeón configuraciones de proxy editamos los campos: puerto utilizado por el proxy ingresamos el 3128. Nombre de equipo visible usado por el proxy ingresamos Denegar. Cuenta de correo usada para notificación (cache admin). Tamaño máximo de subida (saliente en kb) ingresamos 30000.

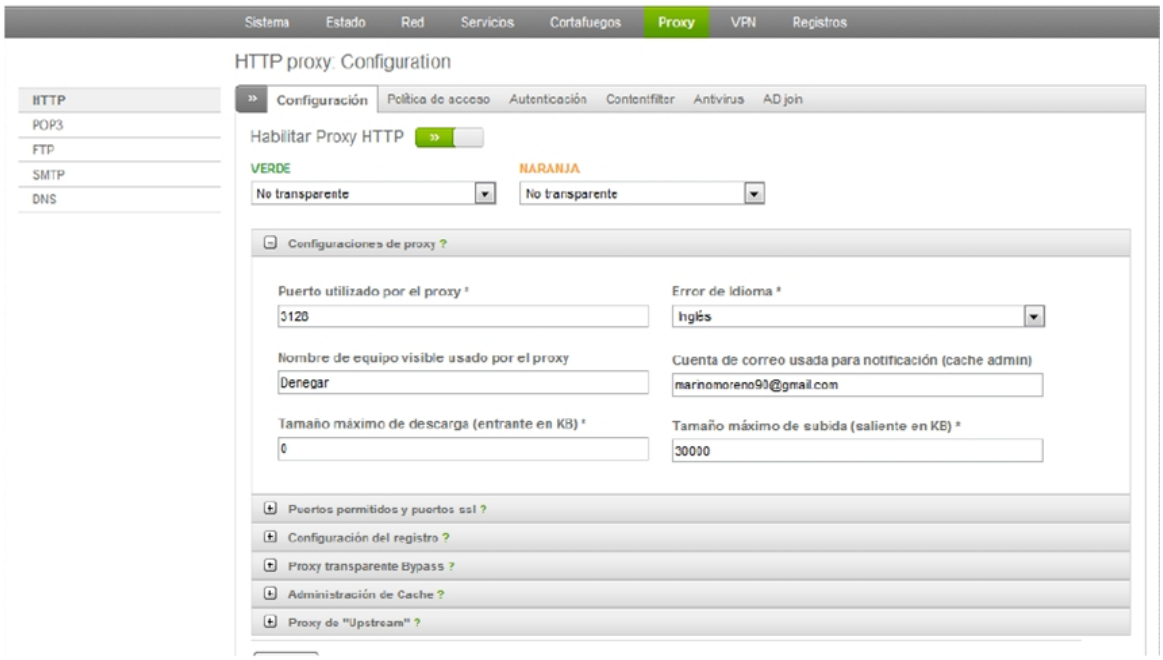

Ilustración 62. Configuraciones de proxy

Haciendo click en la opción puertos permitidos y puertos ssl en el menú tipo acordeón podemos visualizarlos y configurarlos.

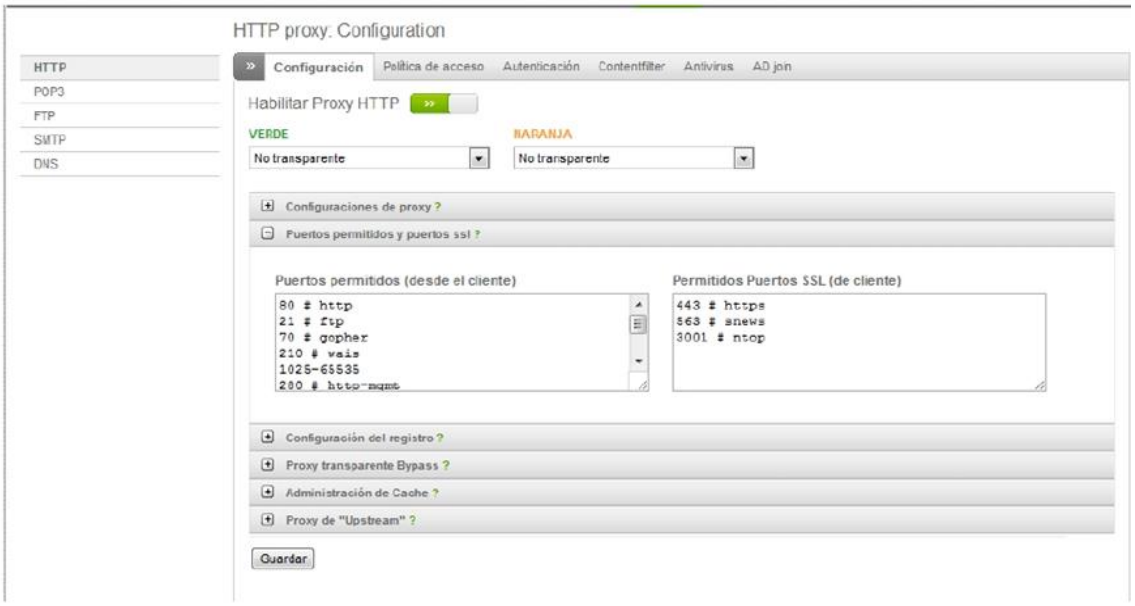

Ilustración 63. Puertos permitidos y puertos ssl

Seleccionamos en el menú acordeón configuración del registro y verificamos que las opciones para logs estén marcadas.

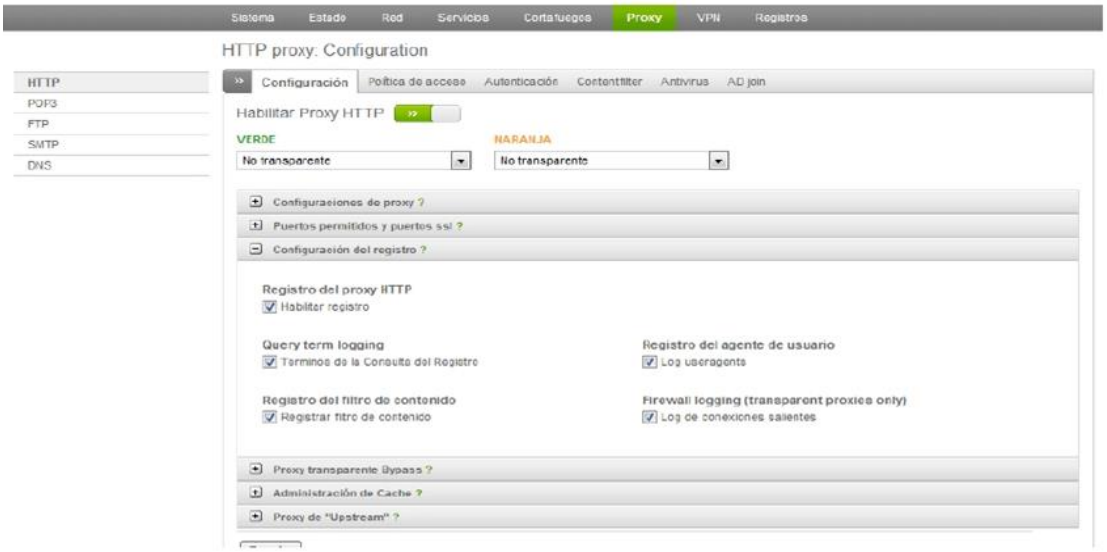

Ilustración 64. Configuración del registro

En la opción proxy transparente bypass la dejamos por defecto.

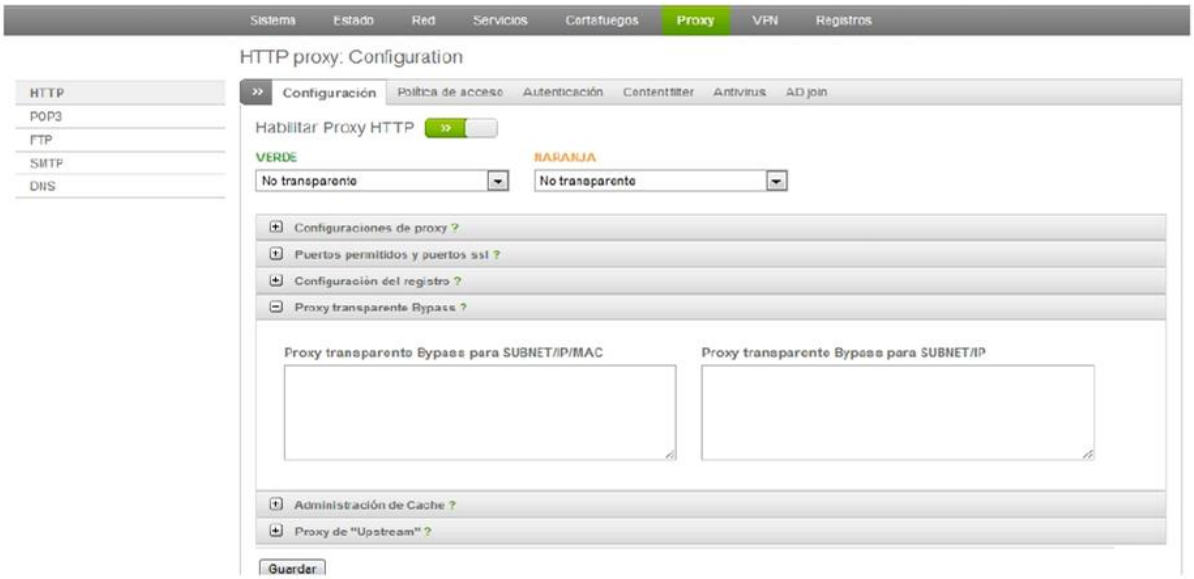

Ilustración 65. Proxy transparente Bypass

Las opciones de administración de cache las dejamos con la configuración por defecto.

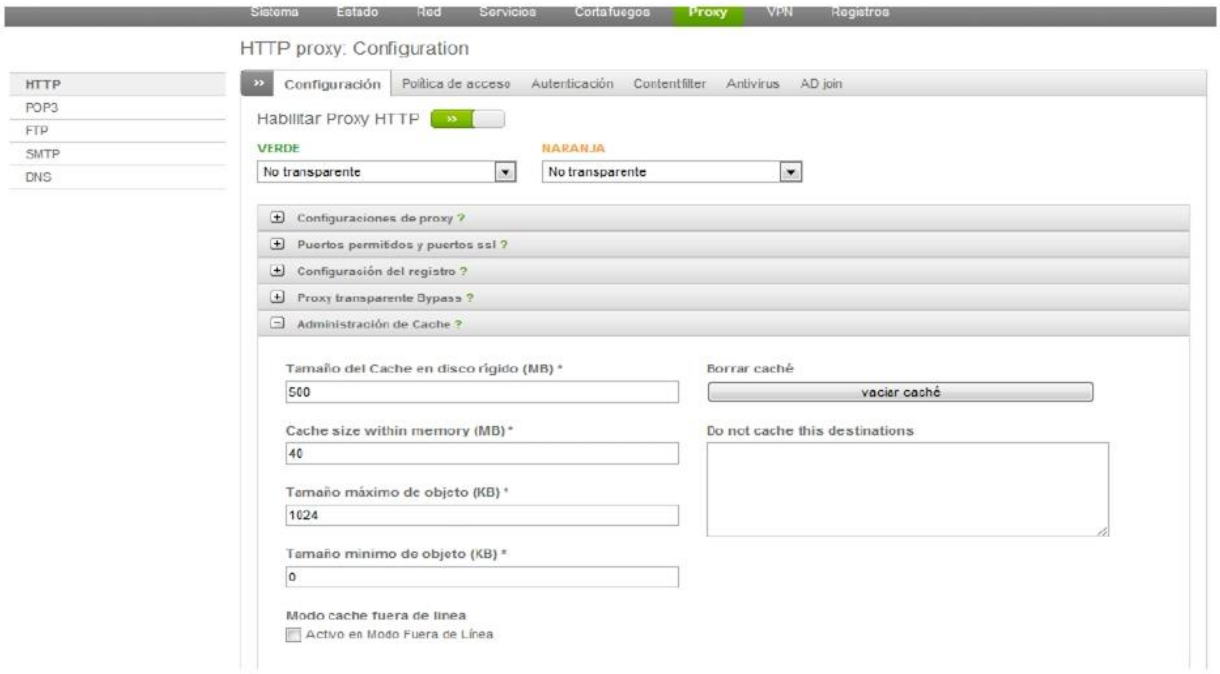

Ilustración 66. Administración cache

Igualmente la opción proxy de upstream.

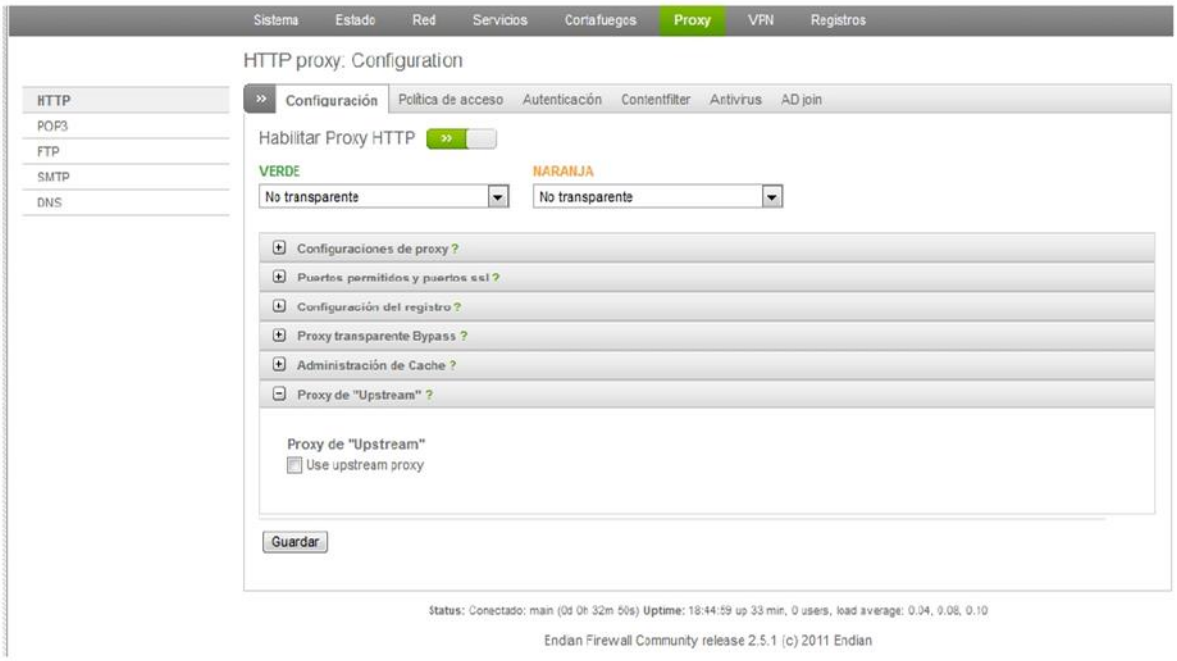

Ilustración 67. Proxy upstream

Guardamos la configuración del proxy.

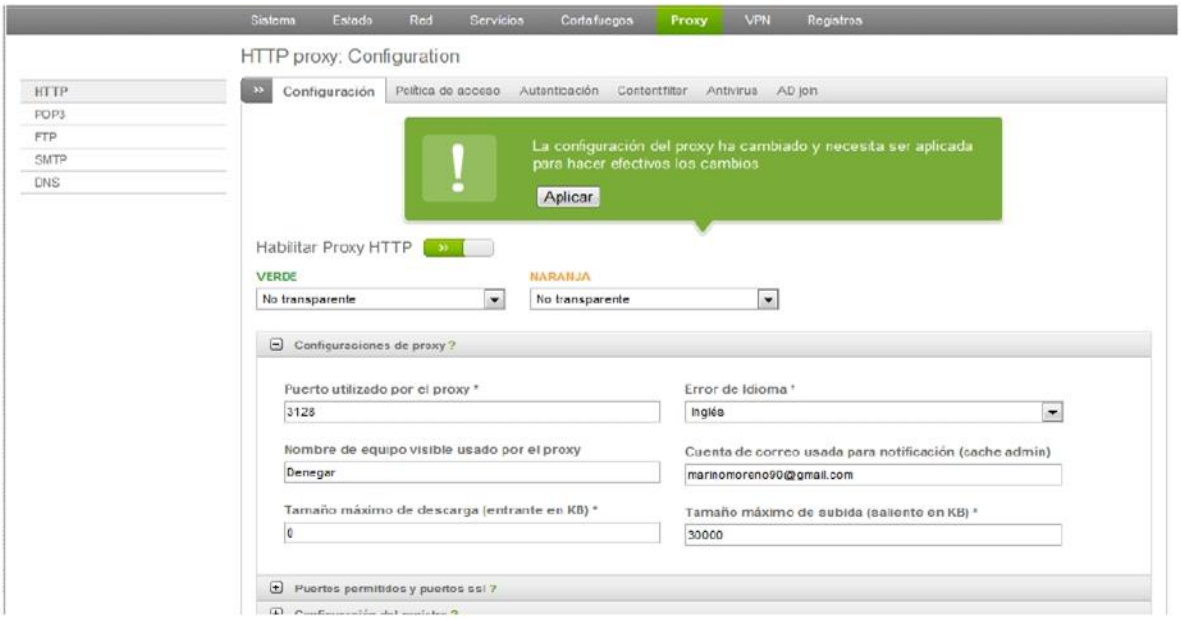

Ilustración 68. Guardar configuración proxy

Aplicamos la configuración del proxy.

Ilustración 69. Aplicar configuración proxy

Ahora lo que vamos a hacer es crear usuarios que se autentiquen en el proxy, para esto seleccionamos la pestaña autenticación.

Ilustración 70. Pestaña autenticación

Pinchamos en el botón administrar usuarios y añadimos usuarios NCSA

Ilustración 71. Añadir usuario NCSA

A continuación llenamos los datos para la creación del usuario.

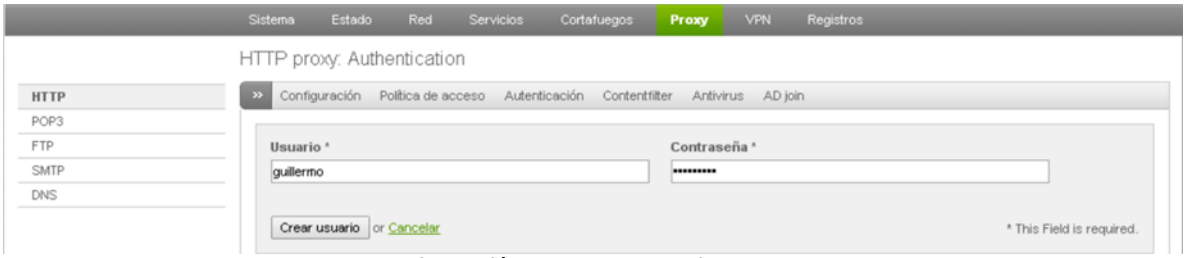

Ilustración 72. Datos usuario NCSA

Creamos el usuario NCSA.

Ilustración 73. Guardar usuario NCSA

Aplicamos el usuario NCSA

Ilustración 74. Aplicar usuario NCSA

A continuación lo que haremos será crear grupos de usuarios, para esto en la pestaña autenticación pinchamos el botón administrar grupos.

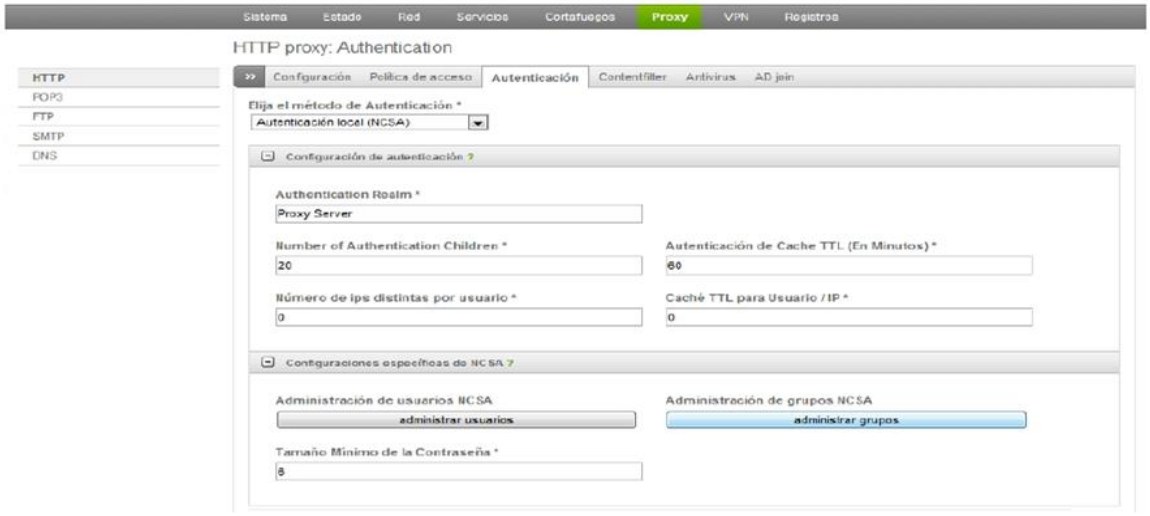

Ilustración 75. Pestaña autenticación - administrar grupos

Seguidamente seleccionamos el enlace añadir grupo NCSA.

Ilustración 76. Añadir grupo NCSA

Suministramos los datos necesarios como nombre del grupo, seleccionamos los usuarios previamente creados que pertenecerán al grupo.

Ilustración 77. Datos grupo NCSA

Guardamos los datos del grupo.

Ilustración 78. Guardar datos grupo NCSA

Aplicamos los datos del grupo.

Ilustración 79. Aplicar datos grupo NCSA

Ahora lo que vamos a hacer es crear los filtros que se aplicaran al contenido que pueden visitar los usuarios. Para esto visitamos la pestaña contentfilter y seguidamente nos dirigimos al enlace crear perfil.

Ilustración 80. Pestaña contenfilter

Nos cargará el siguiente contenido.

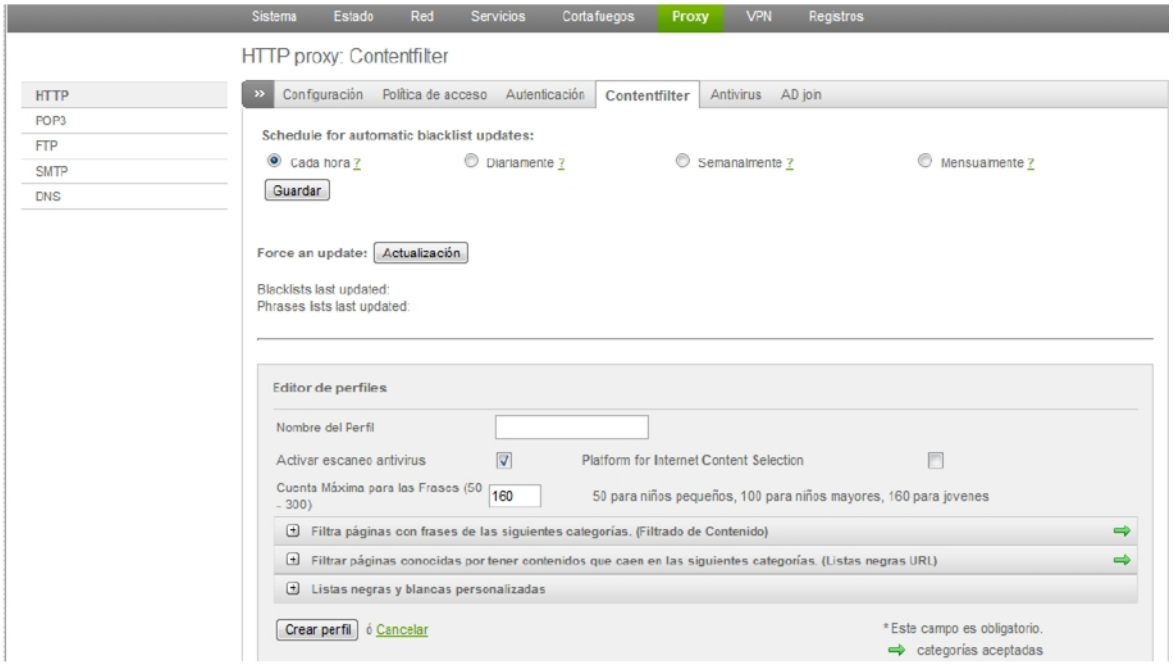

Ilustración 81. Contenfilter crear perfil

Ingresamos el nombre del filtro.

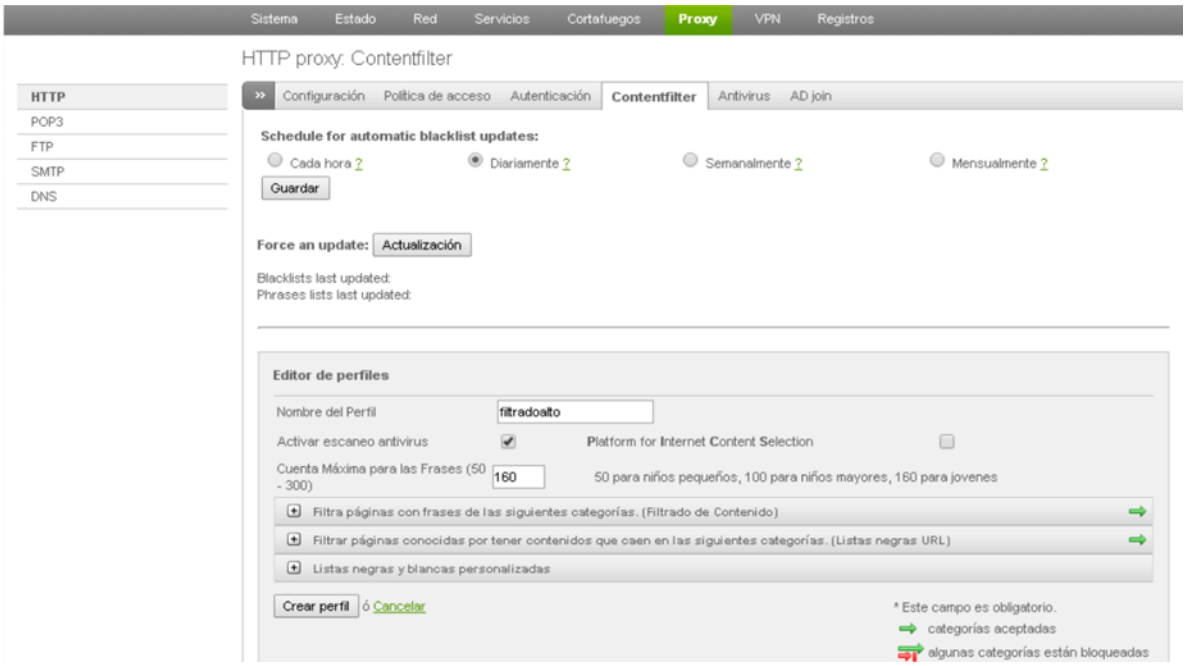

Ilustración 82. Nombre del perfil

Realizamos en la opción de filtrar páginas de las siguientes categorías que es el filtrado de contenido.

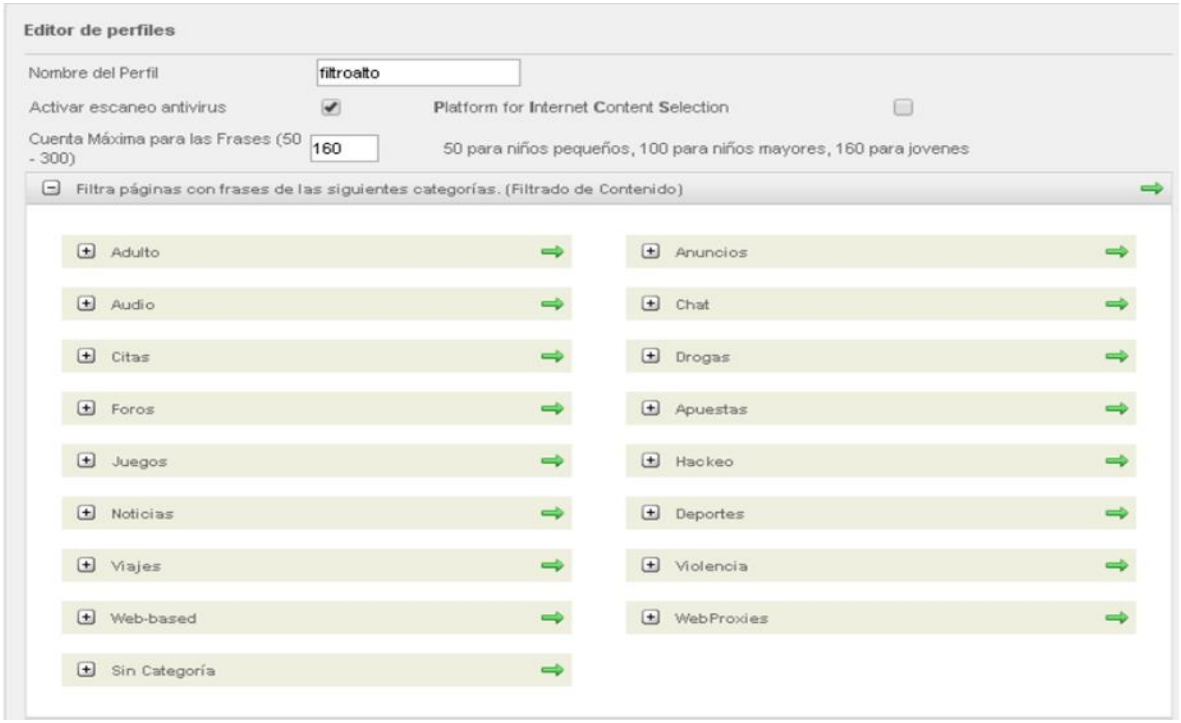

Ilustración 83. Filtrado de contenido Alto

Denegamos el contenido de tipo pornográfico, citas, juegos, deportes, drogas, violencia, chat, etc.

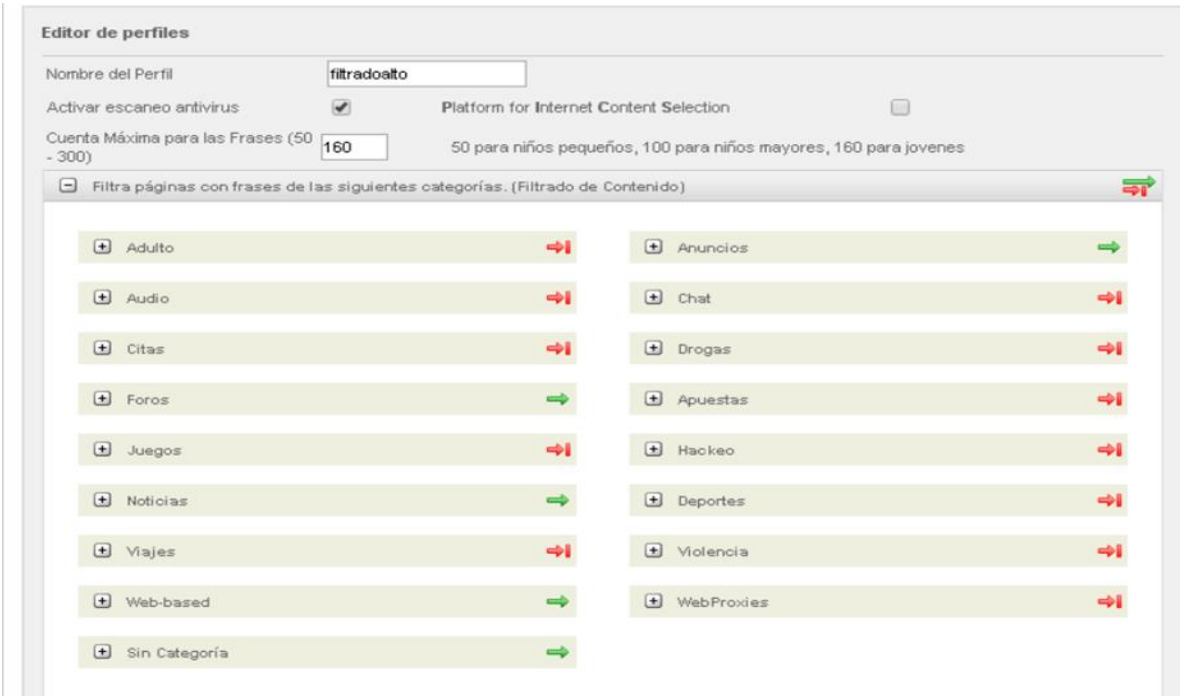

Ilustración 84. Denegar contenido pornográfico y juegos

También podemos filtrar páginas conocidas por tener contenidos que caen en categorías definidas, llamadas listas negras.

Ilustración 85. Listas negras denegar contenido pornográfico, juegos, etc.

Además podemos personalizar las listas negras y listas blancas, en la siguiente figura podemos observar que se denegó el acceso a las páginas de Facebook, twitter, youtube, winsport, rojadireca, etc.

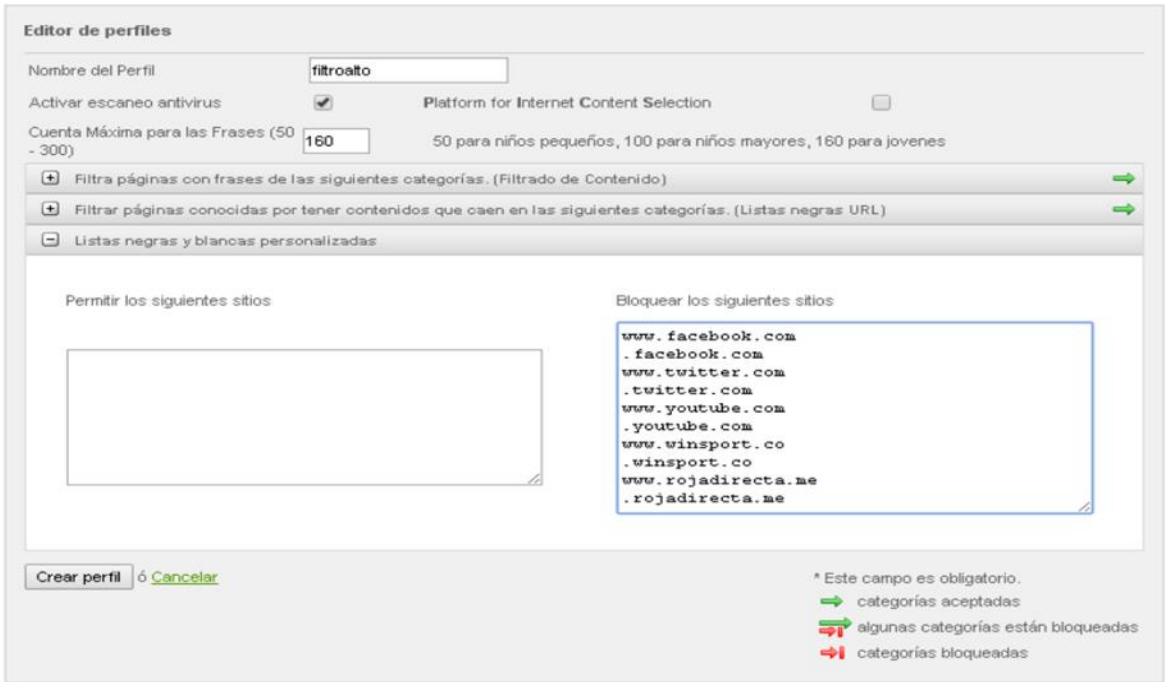

Ilustración 86. Listas negras y listas blancas

Creamos el perfil del filtro de contenido.

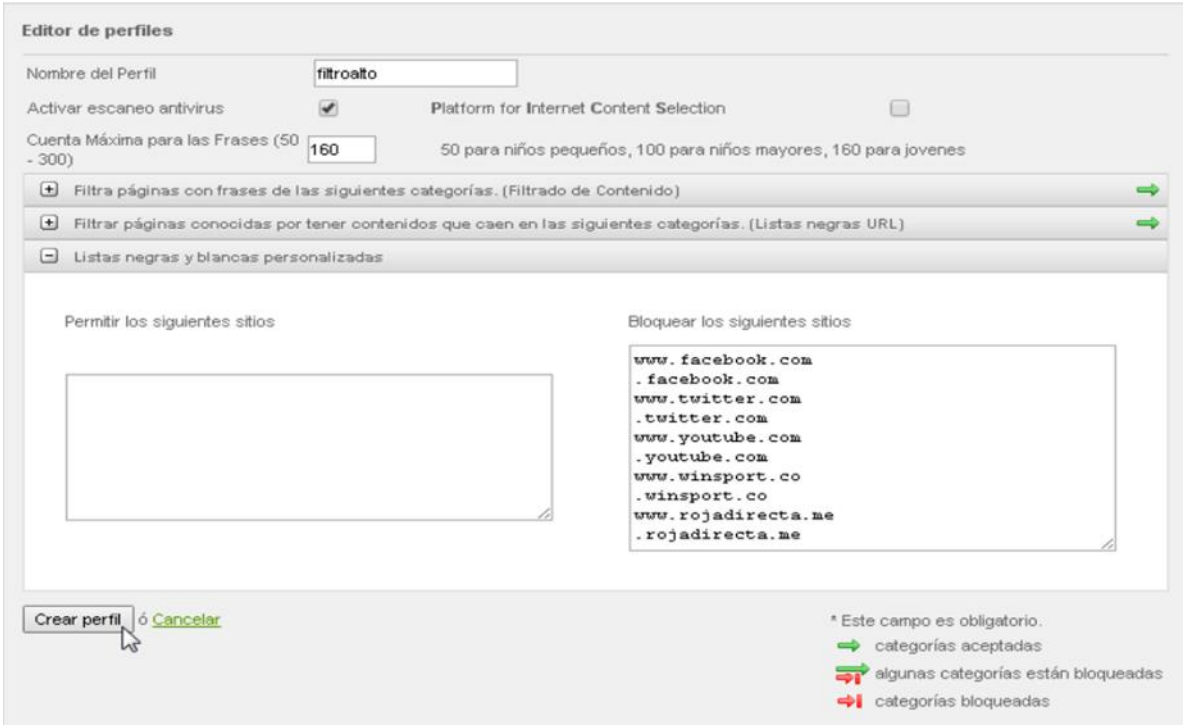

Ilustración 87. Crear perfil listas negras y listas blancas

Aplicamos el filtro de contenido.

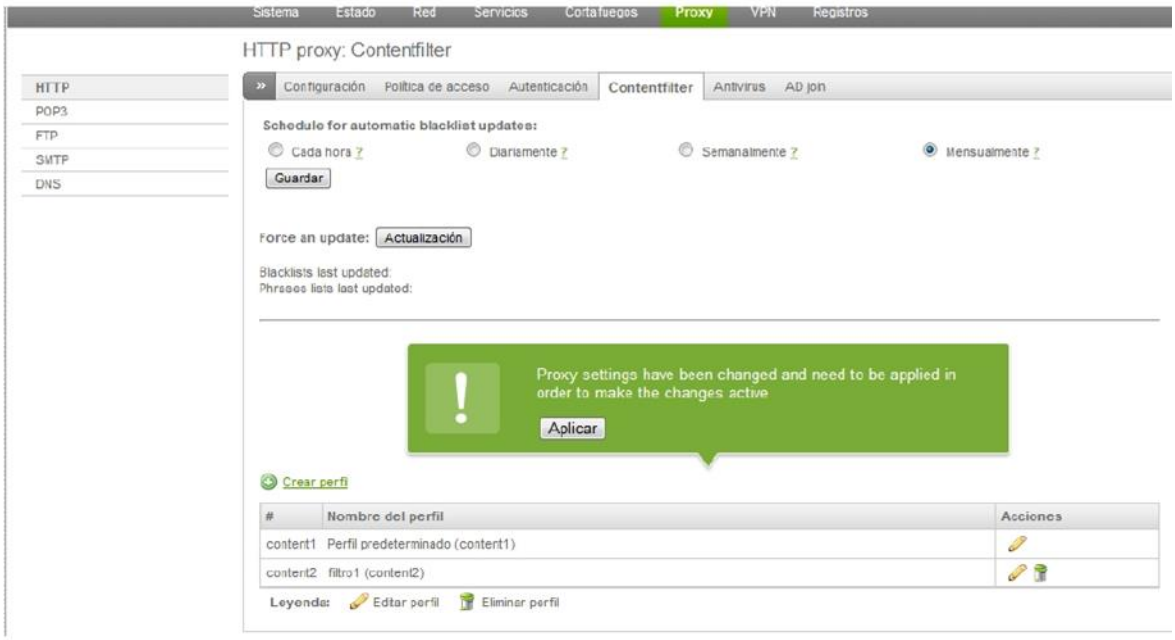

Ilustración 88. Mensaje de creación de perfil

Ilustración 89. Aplicar creación de perfil

Ahora pasaremos a crear la política de acceso, para esto nos dirigimos a la pestaña política de acceso y pichamos el enlace agregar política de acceso.

Ilustración 90. Pestaña política de acceso

Seleccionamos el tipo de fuente y tipo de destino cualquiera, seleccionamos la autenticación basada en usuarios y seleccionamos los usuarios permitidos.

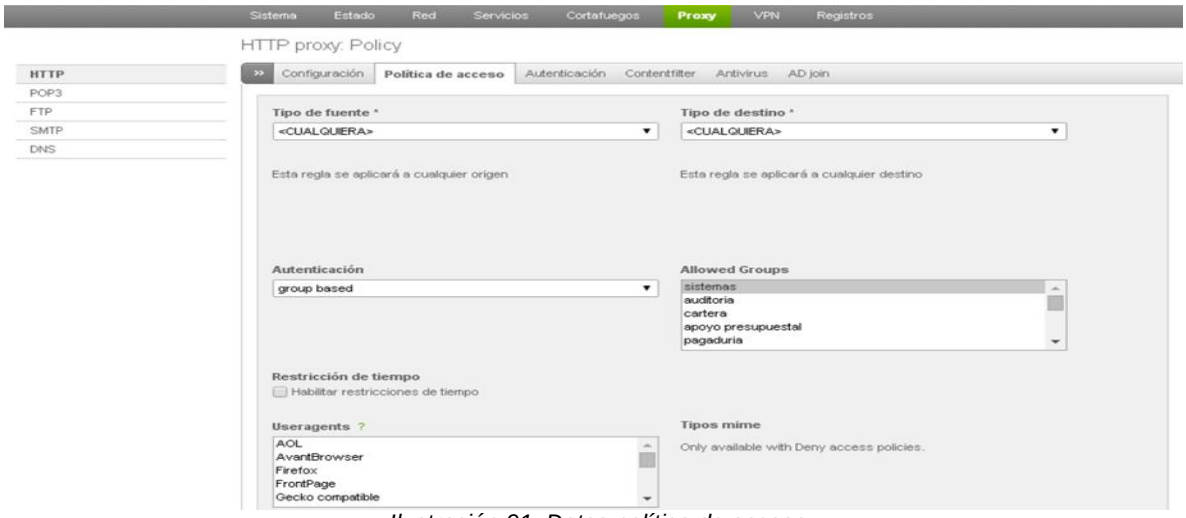

Ilustración 91. Datos política de acceso

A continuación seleccionamos el filtro del perfil que creamos anteriormente.

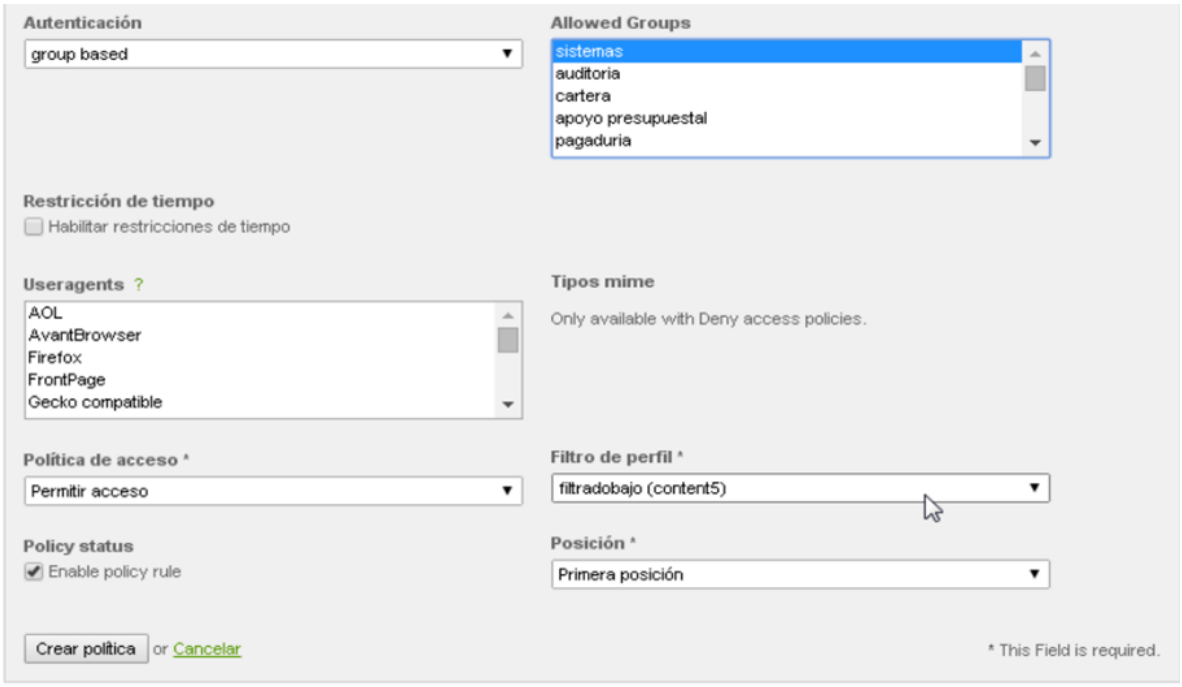

Ilustración 92. Selección de filtrobajo

Creamos la política de acceso

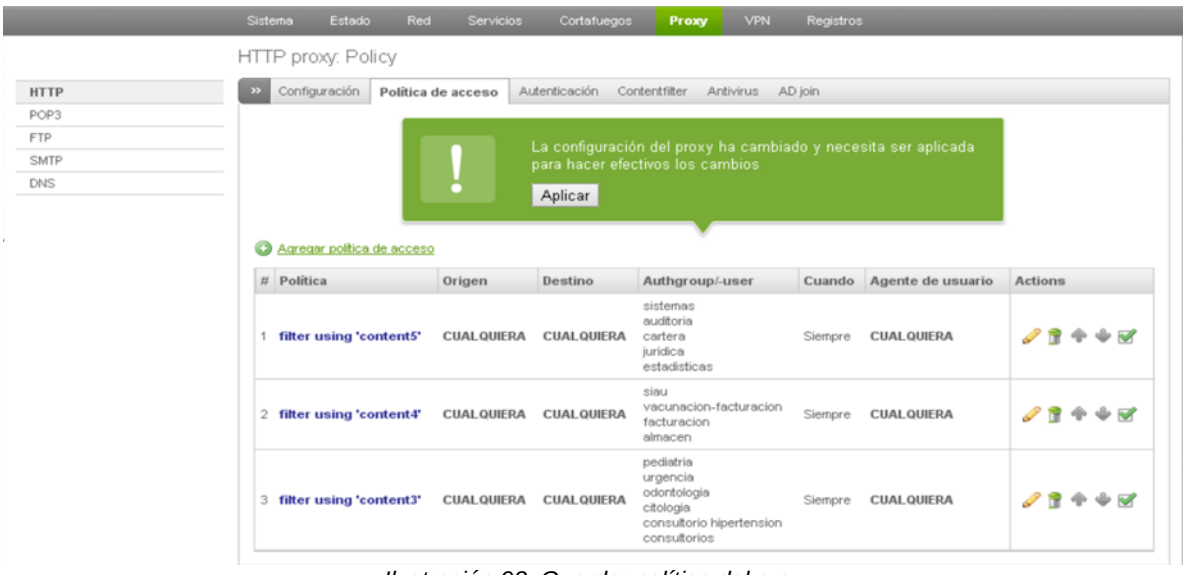

Ilustración 93. Guardar política del proxy

Aplicamos la política de acceso.

Ilustración 94. Aplicar política del proxy

Abrimos un navegador web en este caso mozilla Firefox, en el menú de este seleccionamos herramientas>opciones

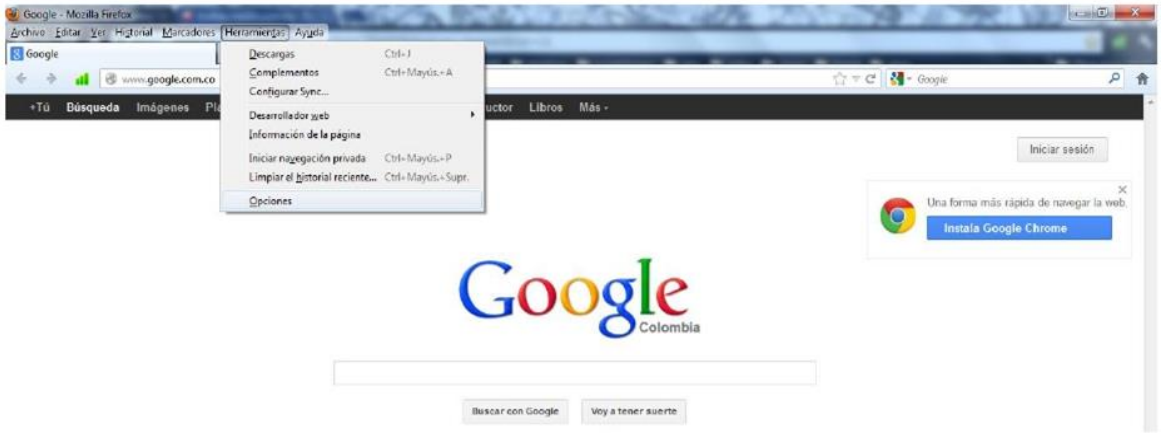

Ilustración 95. Configuración navegador web mozilla

Acontinuación en la ventana que despliega seleccionamos avanzado y la pestaña red y por ultimo configuración.

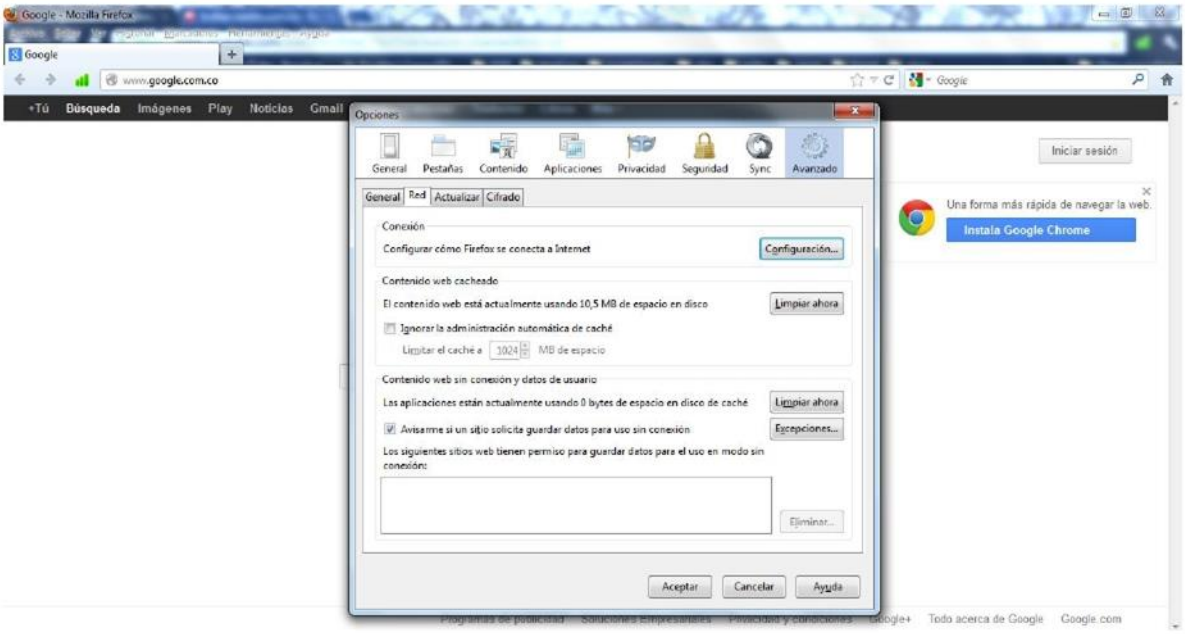

Ilustración 96. Opciones avanzadas - pestaña red

Seleccionamos la opción configuración manual de proxy e ingresamos en proxy http la dirección del servidor 192.168.2.1 por el puerto 3128 que se definió anteriormente en la configuración del servidor proxy. Guardamos la configuración y reiniciamos el navegador.

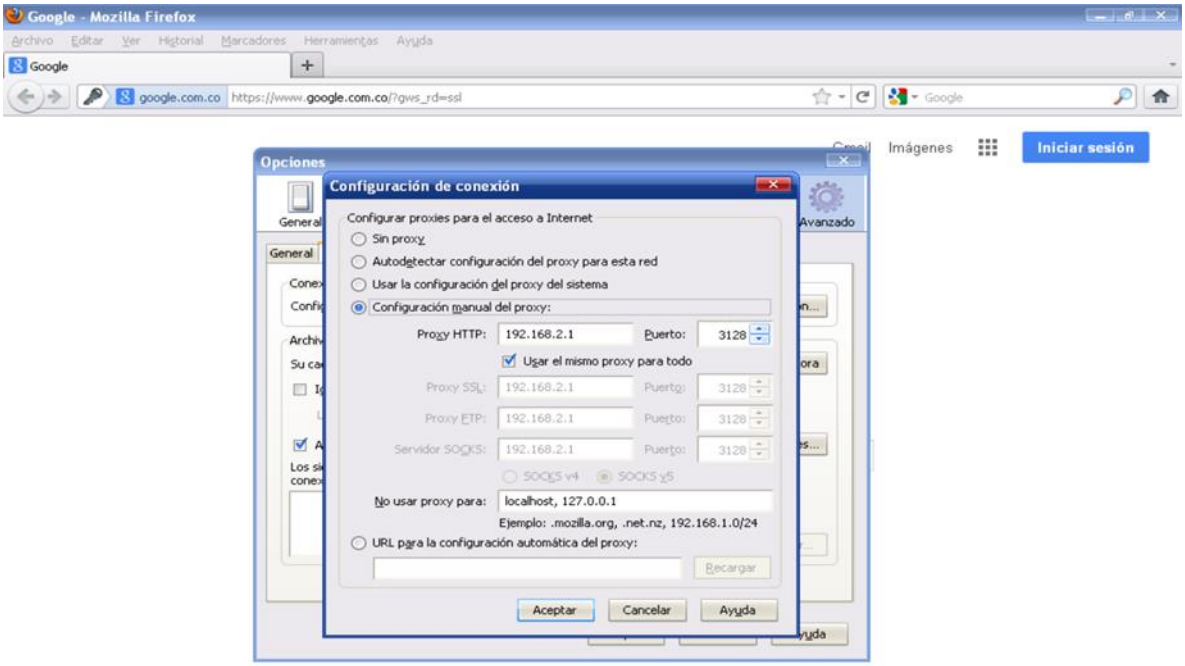

Ilustración 97. Configuración de conexión

El navegador pedirá que nos autentiquemos, ingresamos los datos de la cuenta de usuario que se definió anteriormente.

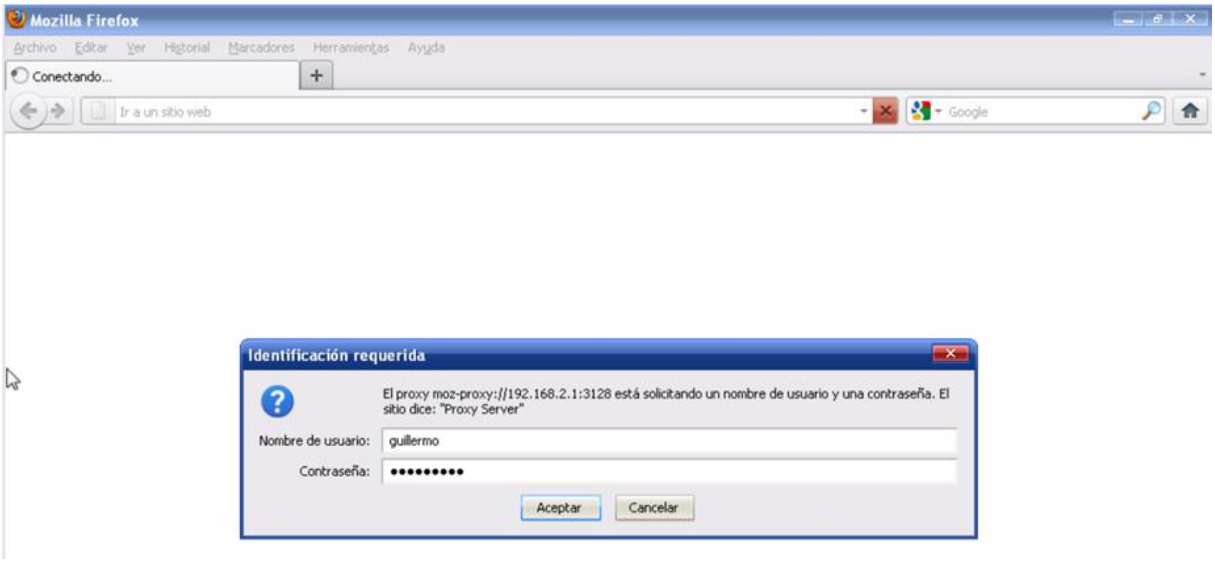

Ilustración 98. Autenticación navegador

Ahora probaremos a abrir las páginas a las cuales se denegó el acceso al usuario. En la siguiente figura se puede observar la restricción a la página de youtube.

Ilustración 99. Denegación youtube

En la siguiente figura se puede observar la restricción a la página de Facebook

Ilustración 100. Denegación Facebook

7. CONCLUSIONES

El contenido de la ISO 27001 está orientado al tratamiento de seguridad de la información mediante la gestión de riesgos, ya que describe la manera de mantener y mejorar la seguridad de los activos de información de cualquier organización.

Para garantizar y mejorar la seguridad en cuanto a la confiabilidad, disponibilidad e integridad de la información en el Hospital San Nicolás, se ha diseñado un Sistema de Gestión de Seguridad de la Información, en donde se ha determinado que algunos activos se encuentran desprotegidos por ende se ha definido controles que aseguren la protección de la información.

Al tener implantado un SGSI bajo la norma ISO 27001 no significa contar con seguridad máxima en la información de la organización sino que esto significa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

Realizar periódicamente el análisis de riesgo y monitorear constantemente la situación, ya que la seguridad que se requiere manejar con un SIGI es permanente para lo cual es necesario un proceso continuo.

Dado que ahora la información es considerada como el activo más importante de la organización es imprescindible protegerlo contra las amenazas que se encuentran en el medio.

Se debe definir y documentar las reglas y derechos de acceso de los recursos del sistema de información para cada usuario o cada grupo de usuarios en una declaración de políticas de acceso. Esta política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos.

Es primordial la metodología y herramienta para el análisis de riesgo, en nuestro caso se optó por la herramienta MSAT debido a las características de la empresa, reconocimiento y por sus lineamientos con la norma ISO/IEC 27001.

Existen diversas herramientas tanto libres como privativas que apoyan el sistema de gestión de seguridad de la información, optimizando procesos o actividades.

Se recomienda revisar continuamente o por lo menos cada seis meses el sistema de gestión de seguridad de la información ya que está en mejora continua.

Debido a que la información es muy importante se recomienda que las empresas capaciten al personal referente a la norma de seguridad informática, y no verlo como un gasto sino como una inversión, ya que son muchos los beneficios obtenidos gracias a la aplicación de esta norma.

8. BIBLIOGRAFIA

Endian UTM Appliance 2.5 Reference Manual. URL http://docs.endian.com/. (Consultada: Junio 20, 2014).

ISO/IEC 27001:2005. 2005. Estándar Internacional. Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de Seguridad de la Información – Requerimientos. 1ra. Edición.

ISO 27001 Security home. URL: http://www.iso27001security.com/index.html. (Consultada: Septiembre 08, 2014).

López, A. 2008. Su portal: El Portal de ISO 27001 en español. (ISO27000.es). URL: http://www.iso27000.es/sgsi.html. (Consultada: Octubre 17, 2013).

Alexander, A. 2011. Análisis y evaluación del riesgo de información: aplicación de la ISO 27001 (2011). URL: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf. (Consultada: Octubre 17, 2014)

Microsoft. 2009. Herramienta de Evaluación de Seguridad de Microsoft (MSAT). URL: https://technet.microsoft.com/es-es/library/cc185712.aspx. (Consultada Noviembre 10, 2014.)

Moreno, M. & López, C. (2013). Análisis y diseño de políticas de seguridad informática aplicadas en redes de datos de pequeñas y medianas empresas (PYMES), caso de estudio: empresa NEXTIN S.A.S.

Bustamante, R. (2010). Seguridad en Redes . URL: http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica.pdf. Consultado (Abril 20, 2015).

Mayol, R. (2006). Modelo para la auditoria de la seguridad informática en la red de datos de la universidad de los Andes. URL: http://tesis.ula.ve/postgrado/tde_busca/arquivo.php?codArquivo=114. Consultado: (Abril 20, 2015).

Ferrer, M. (2006). Firewall software: estudio, instalación y configuración de escenarios y comparativa. URL: http://upcommons.upc.edu/pfc/bitstream/2099.1/3756/2/54344-2.pdf. Consultado: (Abril 20, 2015).

Ladino, M. (2011). Fundamentos ISO 27001 y su aplicación en las empresas. URL: http://www.redalyc.org/articulo.oa?id=84921327061. Consultado: (Abril 21, 2015).

Támara, G. (2006). Firewall-Linux: Una Solución De Seguridad Informática Para Pymes. URL: http://scienti1.colciencias.gov.co:8080/gruplac/jsp/visualiza/visualizagr.jsp?nro=00000000001045. Consultado: (Abril 21, 2015).

Echeverry, J. (2009). Metodología para el diagnóstico continúo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada. URL: http://repository.unimilitar.edu.co/bitstream/10654/10200/1/EcheverryParadaJuanSebastian2009.pdf. Consultado: (Abril 21, 2015).