DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, RED Y VIRTUALIZACIÓN APOYADAS CON SOFTWARE LIBRE EN LA COMPAÑÍA TECNOLOGÍA Y REDES S.A.S.

JAVIER ORLANDO ALARCON VARGAS

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2016

DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, RED Y VIRTUALIZACIÓN APOYADAS CON SOFTWARE LIBRE EN LA COMPAÑÍA TECNOLOGÍA Y REDES S.A.S.

Autor:

JAVIER ORLANDO ALARCON VARGAS

Proyecto de grado presentado para optar al título de
Ingeniero de Sistemas

DIRECTOR:
ING. AUGUSTO ANGEL

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2016

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá D.C., 16 de Noviembre de 2016

Las directivas de la Universidad, los jurados calificadores y el cuerpo docente no son responsables por los criterios e ideas expuestas en el presente documento. Estos corresponden únicamente a los autores.

A Dios, quien representa la culminación de esta gran etapa de mi vida, por hacerlo todo posible y darme fortaleza en cada momento.
A mis padres, por sus incontables sacrificios, su ayuda para alcanzar cada una de mis metas y su inmenso cariño durante todos los días de mi vida.
A mi hijo Tomás, por ser mi motivación y mi fuerza, por alegrar mis días e inundarme de amor.
A mi compañera de vida, Alexandra, por su incondicional apoyo durante todos estos años, por su motivación y sus palabras de aliento, por su inmenso amor, por contagiarme de su optimismo y ser mi fuente principal de inspiración.

Este éxito, no es solo mío, es también de ustedes.

AGRADECIMIENTOS

Se expresa un sincero agradecimiento a las siguientes personas por la colaboración, apoyo incondicional y tiempo durante el inicio, desarrollo y terminación de este trabajo:

A mi familia, por la formación en valores y principios vitales para la culminación de la etapa universitaria.

Al Ingeniero Augusto Ángel, por el acompañamiento, la dedicación, la ayuda y la asesoría brindada para la culminación del proyecto.

Al Ingeniero Edwin Puentes, por brindarme la posibilidad de desarrollar el proyecto de implementación en la compañía Tecnología y Redes Ltda.

Al ingeniero Oscar Cardenas, por su apoyo constante, su asesoría y orientación.

A mis amigos y compañeros, y a todas esas personas que de una u otra forma, hicieron parte de este trabajo, y permitieron que fuera posible su culminación.

CONTENIDO

Lista de Figuras

pág.

Lista de Tablas

pág.

GLOSARIO

ALTA DISPONIBILIDAD: es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.

ARQUITECTURA DE HARDWARE: es el diseño conceptual y la estructura operacional fundamental de un sistema de computadora.

BACKUP: es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

CLÚSTER: se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de hardwares comunes y que se comportan como si fuesen una única computadora.

DATACENTER: Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Latinoamérica.

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

HARDWARE: se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

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

ISCSI: es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3. Otros protocolos en la capa de transporte son SCSI Parallel Interface y canal de fibra.

LAN: red de área local, (del inglés Local Area Network) es la interconexión de uno o varios dispositivos.

SAN: red de área de almacenamiento, en inglés SAN (Storage Area Network), es una red de almacenamiento integral. Se trata de una arquitectura completa que

agrupa los siguientes elementos: Una red de alta velocidad de canal de fibra o iSCSI. Un equipo de interconexión dedicado (conmutadores, puentes, etc), Elementos de almacenamiento de red (discos duros).

SERVIDOR: En informática, un servidor es un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes**.**

SOFTWARE: *equipamiento lógico o soporte lógico* de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

TOPOLOGÍA DE RED: define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

VIRTUALIZACIÓN: En Informática, es la creación -a través de software- de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

RESUMEN

Este documento, plasma la iniciativa de optimización de los procesos de infraestructura tecnológica de la compañía Tecnología y Redes SAS. Para dar cumplimiento a dicho objetivo, se definen lineamientos acoplados con estándares internacionales de buenas prácticas de tecnología (ITIL, COBIT, TOGAF, ISO27001) y con principios vitales de la seguridad de la información (Integridad, confidencialidad, disponibilidad).

Se realiza un análisis minucioso de los procesos actuales (gestión de la información, política de seguridad, servicios de infraestructura), lo cual permite identificar aspectos de mejora y brinda una ruta a seguir para abordar la problemática desde varios frentes (aspectos tecnológicos, aspectos de seguridad, aspectos de operación). Se llega a la conclusión de que la infraestructura tecnológica actual, no cuenta con la capacidad de procesamiento suficiente para satisfacer las necesidades del negocio, no ofrece los niveles de disponibilidad requeridos para lograr el objetivo corporativo y no proporciona un nivel adecuado de seguridad de la información, siendo ésta el activo más valioso de la organización e insumo vital del negocio.

Para dar solución a la necesidad identificada, se propone la implementación de un ESXi para virtualizar la infraestructura de servidores y comunicaciones actual; El diseño de un topología segura de red y la elaboración de una política de seguridad que garantice niveles adecuados de integridad, disponibilidad y confidencialidad de la información; Todo lo anterior, apoyado con herramientas de software libre

Palabras Clave: Seguridad de la información, virtualización, política de seguridad, alta disponibilidad, software libre, topología de red.

ABSTARCT

This document reflects the initiative to optimize the technological infrastructure processes of the company Tecnologia y Redes SAS. To comply with this objective, guidelines are coupled with international standards of good technology practices (ITIL, COBIT, TOGAF, ISO27001) including vital principles of information security such as Integrity, confidentiality and availability).

A thorough analysis of current processes (information management, security policy, infrastructure services) which allows identifying improvement aspects and provides a route to be followed to address the problem from several fronts (technological aspects, Safety and operation). It is concluded that the current technological infrastructure does not have enough processing capacity to meet the needs of the business, does not offer the levels of availability required to achieve the corporate objective and does not provide an adequate level of information security , Being this the most valuable organization asset and vital business input.

In order to solve the identified need, it is proposed to implement an ESXi to virtualize the current server and communications infrastructure; the design of a secure network topology and the elaboration of a security policy that guarantees adequate levels of integrity, availability and confidentiality of the information; all above, supported with free software tools

Keywords: Information security, virtualization, security policy, high availability, free software, network topology.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Implementar un plan integral de optimización de los procesos de infraestructura tecnológica en la compañía Tecnología y Redes SAS, que comprenda la aplicación de políticas de seguridad informática, red y virtualización apoyadas con herramientas de software libre.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar la política de seguridad informática actualmente operativa, procesos de infraestructura y comunicaciones.
- Realizar un análisis técnico y financiero de la solución a implementar.
- Diseñar una topología de red segura y definir la arquitectura de la solución.
- Establecer una política de seguridad acorde a los estándares internacionales de buenas prácticas.
- Implementar las soluciones de seguridad y virtualización.
- Definir un sistema de monitoreo reactivo de infraestructura.

2. INTRODUCCIÓN

2.1 ASPECTOS DE LA INVESTIGACIÓN

La ferocidad del mercado actual, la volatilidad y fragilidad de las economías mundiales y la tendencia cambiante de las necesidades de consumo a nivel general, demandan innovación constante por parte de las organizaciones; El reto es inmenso: servicios cada vez más seguros, confiables y adaptables, puestos a disposición de los usuarios de manera ágil optimizando costos, no es una tarea fácil, lo anterior requiere de la disposición cada vez en mayor medida de investigación y tecnificación de procesos y capacidad de reingeniería constante.

Así mismo, son innegables las bondades que supone la constante evolución de las tecnologías de información y comunicaciones (TIC's) para el entorno empresarial: difusión masiva, procesos de marketing cada vez más efectivos y de mayor alcance y mayor cobertura de los servicios a costos bajos son sólo algunos ejemplos de los innumerables beneficios que se pueden obtener al sacar provecho de la revolución de las TIC's.

Ahora bien, hablando en términos de la importancia de la información como esencia pura e insumo básico de cualquier negocio, se pueden obtener invaluables ventajas al enfocar la cadena de valor y la planeación estratégica en principios internacionales de buenas prácticas, principios estructurados cuya esencia es garantizar la integridad, disponibilidad y confidencialidad de la información: conservación de valores que históricamente se han materializado en el éxito de innumerables organizaciones en un sinnúmero de sectores de la industria.

Pensando en la proyección futura de Tecnología y Redes SAS, en pro de su crecimiento tecnológico y salud financiera, pero sobre todo pensando en amplificar su potencial de mercado, se propuso la implementación de un proyecto de políticas de seguridad informática, red y virtualización de infraestructura, enmarcadas dentro de los estándares de buenas prácticas internacionales y apoyadas con software libre, políticas que se verán reflejadas en la optimización inmediata de los procesos internos de la organización, un crecimiento notable de la utilidad neta, producto del ahorro que representa el cese de la depreciación del hardware, abaratamiento de los costos de energía y capital humano destinado para la administración de los recursos y la disponibilidad constante de los sistemas de la compañía.

Así pues, se presentó una alternativa innovadora y vanguardista, haciendo uso de tecnología de punta y con equipos de alto rendimiento para ambientes corporativos exigentes.

2.2 DESCRIPCIÓN DEL PROBLEMA

Tecnología Y Redes SAS, es una empresa de servicios tecnológicos que ofrece servicios de cableado estructurado, instalación y configuración de redes Windows, instalación y administración de infraestructura tecnológica, seguridad informática, telefonía IP, colocation centre y tercerización de procesos, con domicilio en la Calle 161C# 59-27. Actualmente cuenta con clientes del sector real como QBE Seguros, Brinks de Colombia, Ingeominas, Instituto geográfico Agustín Codazzi y empresas del sector no gubernamental como Global Communities y MSI. El crecimiento exponencial de clientes y personal técnico y administrativo ha creado una necesidad latente de crecimiento y tecnificación de los procesos de infraestructura, toda vez que la capacidad instalada actual no satisface a cabalidad los requerimientos del negocio.

Actualmente la empresa cuenta con 17 clientes contratantes de infraestructura como servicio (IAAS), siendo éste el núcleo de negocio de la compañía.

2.2.1 Identificación del problema. La empresa no cuenta dentro de su arquitectura de infraestructura tecnológica con esquemas de alta disponibilidad para la infraestructura ni para las aplicaciones de negocio, lo cual, en un posible evento catastrófico representaría la parálisis total de la operación, ocasionando serias pérdidas económicas, sanciones pecuniarias y penales, en el caso de incumplimiento de los contratos establecidos para servicios de infraestructura como servicio (IAAS) y Software como servicio (SAAS).

No se cuenta con un servicio de replicación alterna (Datacenter Alterno), lo cual representa un riesgo para la continuidad del negocio y, lógicamente, también supone un riesgo muy alto ante un posible evento catastrófico.

Tampoco cuenta con lineamientos de arquitectura empresarial bien definidos, que obedezcan a estándares internacionales de buenas prácticas de IT (TOGAF, ITIL V3), lo cual representa un riesgo de calidad al momento de desplegar servicios al ambiente productivo.

En cuanto a calidad en la seguridad de la información, no se cuenta con políticas de acceso eficaces que garanticen la disponibilidad, integridad y confidencialidad de la información; no existe una política de control de acceso a la información y los esquemas de seguridad perimetral no satisfacen las necesidades del negocio.

No se cuenta con un plan de continuidad de negocio (BCP) ni tampoco con un plan de recuperación de desastres (DRP), esto supone un riesgo en sí mismo e incrementa la probabilidad de sanciones pecuniarias y penales.

Los servicios de red básicos, cómo el Directorio Activo, DHCP y DNS reposan todos en un solo servidor que no cuenta con replicación, en caso de una falla de

hardware o sistema operativo, todos los servicios de la compañía quedarían fuera de línea.

Las comunicaciones, servicios de seguridad perimetral, el proxy de navegación hacia internet y las listas de acceso están soportadas en un appliance de firewall (Dlink DFL 260) que no satisface (ni por performance ni por funcionalidad) las necesidades actuales de la organización y tampoco cuenta con sistema de replicación. En caso de fallas de hardware. Los servicios de la compañía y las comunicaciones con los clientes quedarían fuera de línea.

La empresa está conformada por 187 empleados, entre personal técnico de sitio, personal administrativo, personal comercial y directivos. Se detalla a continuación el inventario actual de aplicaciones que se encuentran en producción en la organización:

- **QuickBooks**: Sistema de gestión contable, se implementa en la organización para reportar los cierres fiscales y facturación anual.

- **SIIGO:** Aplicación de gestión contable, soporta el total de la operación financiera.

- **Cimco Plus:** Aplicación para la gestión de crédito y cartera, utilizada en para la gestión de la cartera corporativa.

- **Novasoft**: Aplicación de gestión de nómina,

- **Visor**: Aplicación para la gestión de archivos digitales, contiene las evidencias históricas de las operaciones financieras y contables de la organización.

- **Antivirus**: Se cuenta con el producto Symantec Endpoint Protection 12.1 en modo consola, desde donde se administran los paquetes instalados en las estaciones de trabajo.

- **Help Desk (MantisBT):** Sistema de mesa de ayuda, que se usa de manera interna para la gestión de requerimientos, pero que también interactúa con los clientes con el mismo fin.

Así las cosas y teniendo en cuenta la necesidad actual, se pretende implementar una solución integral, disponible, segura y que se adapte a los recursos financieros existentes, por lo cual se propone una combinación de software propietario y software libre, optimizando costos sin poner en riesgo la continuidad de la operación diaria de la compañía.

2.3 JUSTIFICACIÓN DEL PROYECTO DE IMPLEMENTACIÓN

La necesidad de optimizar los procesos de infraestructura tecnológica, seguridad de la información y definir un plan de continuidad de negocio, optimizando la gestión de los recursos financieros, de tiempo y operativos, hacen primordial la implementación del proyecto de investigación.

Se propone una solución que incluye el diseño de una topología segura de red, una política de seguridad acorde con los estándares internacionales de buenas prácticas de IT (ITIL V3, COBIT, ISO27001), virtualización de la infraestructura actual en una arquitectura de alta disponibilidad y el diseño de planes de continuidad de negocio y recuperación de desastres, todo lo anterior apoyado en los principios y lineamientos del software libre.

Siendo abordado desde el concepto de seguridad de la información, la implementación de la solución propuesta ofrecerá **disponibilidad** de la información, al establecer esquemas de alta disponibilidad de los servicios de infraestructura y aplicaciones; **integridad** de la información, gracias al diseño de una política de seguridad sólida que cumple con estándares internacionales de buenas prácticas de IT (ITIL V3, COBIT, ISO27001) e **integridad** de la información, soportada en el diseño de una topología de red segura, con soluciones de seguridad con cortafuegos perimetral y de borde (arquitectura Back End – Front End), que garantiza almacenamiento de datos libres de modificaciones no autorizadas.

Por último, la implementación de la solución propuesta, permitirá abaratar los costos de administración de la infraestructura, ofreciendo flexibilidad y alta tolerancia a fallas.

3. MARCO TEÓRICO

3.1 BUENAS PRÁCTICAS, ESTÁNDARES Y NORMAS.

"La seguridad de la información es parte activa de nuestra actualidad": La anterior frase ilustra el momento que enfrentamos actualmente en diferentes entornos como el laboral, el educativo y cada vez más, en el hogar. Términos como copia de seguridad, privacidad, antivirus, cifrado, son con el paso de los días parte de nuestro léxico y lo seguirán siendo aún más con la popularización del uso de recursos tecnológicos en casi todos los entornos y espacios.

En la medida que se trabaja inmerso en el mundo de la seguridad de la información y la seguridad informática, aumenta la necesidad de difundir la educación en estos temas; sin embargo, en espacios laborales o educativos no es tan simple como el compartir con un amigo y decirle qué antivirus emplear o cómo proteger su teléfono celular del robo de información. Por ello, es necesario buscar guías y documentos que ilustren cómo abordar la seguridad de una forma responsable, procedimental y orientada al cumplimiento de los estándares mínimos requeridos para la tecnología actual.

Pero surge una duda, ¿qué es un estándar y por qué son tan mencionados en la actualidad? Pues bien, un estándar es un documento con un contenido de tipo técnico-legal que establece un modelo o norma que refiriere lineamientos a seguir para cumplir una actividad o procedimientos. Su uso se ha popularizado en la actualidad debido a que se busca que los procesos y actividades de organizaciones y sus personas sean repetibles, organizados, y estructurados. Por ello, entidades como ISO (International Standard Organization), IEEE (Institute of Electrical and Electronics Engineers), entre otras proponen estos documentos, los cuales se crean a partir de la experiencia de diferentes grupos que participan durante el proceso de definición y al finalizar son documentos de tipo público.

¿QUÉ SE PUEDE ENCONTRAR?

A continuación se detallan algunos estándares internacionales, guías y manuales de buenas prácticas que en la actualidad son ampliamente empleados para buscar el aseguramiento de la información, el activo más valioso de toda organización, en el constante proceso de la consecución de protección a nivel de integridad, disponibilidad y confidencialidad[1].

- **ISO/IEC 27001:** Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de

[1] BORBÓN SANABRIA, Jeffrey Steve. Buenas prácticas, estándares y normas [en línea] Revista Seguridad 1 251 478 [Citado Julio 25, 2011] Nº 11. Disponible en internet: http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI)[2].

Los beneficios que aporta el estándar a la organización son los siguientes:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora[3].

- **ISO/IEC 27002:** Es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013. En términos generales, la norma cuenta con las siguientes directrices:

  ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

[2] WIKIPEDIA. Definición ISO/IEC 27001 [en línea] [Citado Septiembre 14, 2011] Disponible en internet: https://es.wikipedia.org/wiki/ISO/IEC_27001

[3] COTECNA Trade Services. Certificación ISO 27001 [en línea] Disponible en internet_ http://www.cotecna.com.ec/~/media/Countries/Ecuador/Documents/Brochure-iso-27001-cotecna-ecuador-FINAL.ashx?la=es-ES

La versión de 2013 del estándar describe los siguientes catorce dominios principales:

- Organización de la Seguridad de la Información.
- Políticas de Seguridad
- Seguridad de los Recursos Humanos.
- Gestión de los Activos.
- Control de Accesos.
- Criptografía.
- Seguridad Física y Ambiental.
- Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.
- Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.
- Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
- Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.
- Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.
- Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.
- Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades[4].

- **ISO/IEC 27005:** Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

  ISO/IEC 27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.

[4] WIKIPEDIA. Definición ISO/IEC 27002 [en línea] [Editado Mayo 8, 2016] Disponible en internet: https://es.wikipedia.org/wiki/ISO/IEC_27002

Los usuarios elijen el método que mejor se adapte para, por ejemplo, una evaluación de riesgos de alto nivel seguido de un análisis de riesgos en profundidad sobre las zonas de alto riesgo. La norma incorpora algunos elementos iterativos, por ejemplo si los resultados de la evaluación no son satisfactorios. ISO 27005 sustituyó a la Gestión de la Información y Comunicaciones Tecnología de Seguridad, la norma ISO / IEC TR 13335-3:1998 y la norma ISO / IEC TR 13335-4:2000.Las secciones de contenido son:

- Prefacio.
- Introducción.
- Referencias Normativas.
- Términos y condiciones.
- Estructura.
- Fondo.
- Descripción del proceso de ISRM.
- Establecimiento de contexto.
- Información sobre la evaluación de riesgos de seguridad (ISRA).
- Tratamiento de riesgos de seguridad de la información.
- Admisión de riesgos de seguridad de la información.
- Comunicación de riesgos de seguridad de la información.
- Información de seguridad, seguimiento de riesgos y revisión.
- Anexo A: Definición del alcance del proceso.
- Anexo B: Valoración de activos y evaluación de impacto.
- Anexo C: Ejemplos de amenazas típicas.
- Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
- Enfoques ISRA: Anexo E.

Se trata de un estándar que cuenta con una parte principal concentrada en 24 páginas, también cuenta con anexos en los que se incluye ejemplos y más información de interés para los usuarios.

En estos anexos reposan amenazas, vulnerabilidades e impactos, lo que puede resultar útil para abordar los riesgos relacionados con los activos de la información en evaluación[5].

- **COBIT (Control Objectives for Information and related Technology).**
  Es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición on-line estuvo disponible en 2003); y la cuarta edición en diciembre de 2005, y la versión 4.1 está disponible desde mayo de 2007.

[5] SGSI. ISO/IEC 27005 Gestión de Riesgos de la Seguridad la información [en línea] Blog especializado en sistemas de gestión de seguridad de la información [Citado Enero 31, 2014] http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

COBIT 4.1
En su cuarta edición, COBIT tiene 34 procesos que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios:

- Planificación y Organización (Plan and Organize).
- Adquisición e Implantacion (Acquire and Implement).
- Entrega y Soporte (Deliver and Support).
- Supervisión y Evaluación (Monitor and Evaluate).

COBIT 5.
Isaca lanzó el 10 de abril de 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del framework mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

COBIT 5 se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros importantes marcos y normas como Val IT y Risk IT, Information Technology Infrastructure Library (ITIL ®) y las normas ISO relacionadas en esta norma.

Beneficios
COBIT 5 ayuda a empresas de todos los tamaños a:
- Optimizar los servicios el coste de las TI y la tecnología
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas
- Gestión de nuevas tecnologías de información.

Misión
La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores". Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información [6].

- **ITIL (Information Technology Infrastructure Library)**

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un conjunto de conceptos y buenas prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

[6] WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas [en línea] [Editado Abril 19, 2016] Disponible en internet: https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

Historia

Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. Esta mayor adopción y conocimiento ha llevado a varios estándares, incluyendo ISO/IEC 20000, que es una norma internacional cubriendo los elementos de gestión de servicios de TI de ITIL. ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la Information Services Procurement Library (ISPL, 'Biblioteca de adquisición de servicios de información'), la Application Services Library (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, Dynamic Systems Development Method), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la información mediante COBIT (Control OBjectives for Information and related Technology).

El concepto de gestión de servicios de TI, aunque relacionado con ITIL, no es idéntico: ITIL contiene una sección específicamente titulada «Gestión de Servicios de TI» (la combinación de los volúmenes de Servicio de Soporte y Prestación de Servicios, que son un ejemplo específico de un marco ITSM). Sin embargo es importante señalar que existen otros marcos parecidos. La Gestión de Servicio ITIL está actualmente integrada en el estándar ISO 20000 (anterior BS 15000).

ITIL se construye en torno a una vista basada en proceso-modelo del control y gestión de las operaciones a menudo atribuida a W. Edwards Deming. Las recomendaciones de ITIL fueron desarrolladas en los años 1980 por la Central Computer and Telecommunications Agency (CCTA) del gobierno británico como respuesta a la creciente dependencia de las tecnologías de la información y al reconocimiento de que sin prácticas estándar, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y duplicaban esfuerzos dentro de sus proyectos TIC, lo que resultaba en errores comunes y mayores costes.

ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e IT Infrastructure Library (Biblioteca de infraestructura de TI) son marcas registradas de la Office of Government Commerce (Oficina de comercio gubernamental, OGC), que es una división del Ministerio de Hacienda del Reino Unido.

En abril de 2001 la CCTA fue integrada en la OGC, desapareciendo como organización separada.

En diciembre de 2005, la OGC emitió un aviso de una actualización a ITIL, conocida comúnmente como ITIL v3, que estuvo planificada para ser publicada a finales de 2006; habiendo sido realizada en junio de 2007. Se esperaba que la publicación de ITIL versión 3 incluyera cinco libros principales, concretamente: Diseño de Servicios de TI, Introducción de los Servicios de TI, Operación de los Servicios de TI, Mejora de los Servicios de TI y Estrategias de los Servicios de TI, consolidando buena parte de las prácticas actuales de la versión 2 en torno al Ciclo de Vida de los Servicios.

Uno de los principales beneficios propugnado por los defensores de ITIL dentro de la comunidad de TI es que proporciona un vocabulario común, consistente en un

glosario de términos precisamente definidos y ampliamente aceptados. Un nuevo glosario ampliado ha sido desarrollado como entregable clave de ITIL versión 3[7].

ITIL V3.
En ITIL v3 reestructura el manejo de los temas para consolidar el modelo de "ciclo de vida del servicio" separando y ampliando algunos subprocesos hasta convertirlos en procesos especializados. Esta modificación responde a un enfoque empresarial para grandes corporaciones que utilizan ampliamente ITIL en sus operaciones y aspira a consolidar el modelo para conseguir aún mejores resultados. Es por ello que los especialistas recomiendan que empresas emergentes o medianas no utilicen ITIL v3 si no cuentan con un modelo ITIL consolidado y aspiran a una expansión a muy largo plazo. ITIL v3 consta de 5 libros basados en el ciclo de vida del servicio:

- Estrategia del Servicio
- Diseño del Servicio
- Transición del Servicio
- Operación del Servicio
- Mejora Continua del Servicio[8]

3.2 SEGURIDAD INFORMÁTICA Y SOFTWARE LIBRE

Habitualmente los usuarios finales no tienen en consideración la seguridad cuando hacen uso de un sistema, ya que, frecuentemente se ignoran los aspectos relacionados con la seguridad. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la seguridad suele ir en el platillo opuesto de la comodidad y facilidad de uso en la balanza del diseño de un sistema. Es por esto que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe su capacidad de realización de un trabajo determinado. En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas (como por ejemplo, recordar contraseñas, cambiarlas periódicamente, etc.) y que pueden limitar las operaciones que puede realizar así como los recursos a los que se le permite acceder.

Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico. Por ejemplo, cuando se guardan cosas en una caja fuerte en un banco real, no se piensa que cualquier persona del mundo puede llegar a ésta de una forma inmediata como si se tratara, en lugar de un banco, de

[7] WIKIPEDIA. Information Tecnology Infraestructure Library [en línea] [Editado Junio 7, 2016] Disponible en internet: https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Historia_y_precursores_de_ITIL

[8] CAPACITACIÓN ITL. Itil versión 3 [en línea] ITIL V3 [Citado Junio 7, 2016] Disponible en internet: capacitacionitil.blogspot.com/p/itil-v3-en-itil-v3-reestructura-el.html

una estación de autobuses. En el mundo intangible de la informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Es más, estos usuarios, en el caso de una red global, se cuentan por millones. Algunos serán “buenos vecinos” pero otros serán agentes hostiles.

¿Por qué son necesarios los mecanismos de seguridad?
Para poner de relevancia lo comentado en los párrafos anteriores se han elegido tres casos genéricos que se describen a continuación. Con ellos se pretende mostrar alguno de los peligros, relativos a seguridad, de estar ’interconectados’. Para cada uno de ellos existen mecanismos de seguridad que permiten llevar a cabo las operaciones de manera satisfactoria.

- **Intercambio de Información**

Cuando se intercambia información con un ordenador remoto, esa información circula por una serie de sistemas intermedios que son desconocidos a priori (excepto en ámbitos muy específicos). Además, no sólo no se sabe cuáles serán estos sistemas intermedios, sino que además no se dispone de ningún control sobre ellos o sobre lo que puedan hacer con nuestros datos al pasar por ellos. Quizá el propietario original es de fiar pero su sistema ha sido comprometido por un atacante que toma posesión de los datos enviados.

Por otro lado tampoco se puede estar seguro de que el sistema al que uno se está conectando es quien dice ser. Existen diversos medios técnicos para suplantar la identidad de un sistema y engañar a un tercero cuando realiza la conexión.

En definitiva, no existe una certeza absoluta de que aquellos sistemas a los que uno envíe información sean realmente los auténticos; además, en el caso de que lo sean no se sabe si les llegará la información que se les envía, o si llegará sin cambios o si, aún si llega sin modificaciones, será leída por terceras partes.

- **Instalación de software dañino involuntariamente**

Otra posibilidad que no se debe descartar es que se instale software en un ordenador sin conocimiento del usuario o administrador. Esto puede ocurrir de muchas formas, algunas relacionadas con operaciones que se realizan todos los días. Algunos ejemplos son:

  - Introducción de virus o troyanos por la descarga y ejecución de ficheros en servidores, en principio, confiables, por parte del usuario. El efecto de distribución puede ser, incluso, involuntaria si se hace uso de sistemas de archivos compartidos. En el caso de los virus el efecto destructivo se hará patente más pronto o más tarde. La instalación de troyanos puede, sin embargo, pasar desapercibida.

- Difusión de virus por correo electrónico. Lograda gracias a la malversación por parte del virus del programa utilizado como lector de correo (que lo ejecuta automáticamente sin intervención del usuario) o porque el usuario activa el virus inadvertidamente creyendo que se trata de otra cosa. Su efecto pernicioso es, además del destructivo habitual de un virus, la distribución a las direcciones conocidas convirtiendo su propagación en exponencial.
- Explotación de una vulnerabilidad de un servicio que se está ofreciendo a través de Internet. Como por ejemplo un servidor web. Un caso similar sería una carpeta compartida donde otros miembros de la red local (y quizá un virus que haya en sus ordenadores) pueden copiar archivos.
    - Este software dañino no sólo puede obtener o borrar información del sistema en el que se instala, también puede servir como plataforma de ataque a otros sistemas.
    - Es por esto que todo ordenador, máxime cuando se encuentra expuesto a recibir información del exterior, debe protegerse con las medidas de seguridad adecuadas aunque se considere que no tiene información ni servicios de gran importancia.

- **Protección ante accesos no autorizados**

Cuando se ofrecen servicios o información en una red para sus usuarios legítimos, al mismo tiempo se abre la puerta a posibles intrusos en estos sistemas. Protegerse de esta posibilidad implica tener un especial cuidado con todo el software empleado, desde el sistema operativo hasta la última de las aplicaciones instalada, y cuidar en gran medida su configuración.

Pero tampoco debería olvidarse la posibilidad de que existan intrusos que accedan físicamente al sistema. La evolución de las comunicaciones ha hecho que se preste una gran atención a la posibilidad de accesos remotos, pero de nada sirve evitar esta posibilidad si se permite el acceso físico al sistema a personas no autorizadas. Es por esto que, en algunos casos pueda ser necesario tomar las medidas de seguridad adecuadas sobre el propio hardware para evitar robos, o pérdidas de información por estos accesos inadecuados.

En definitiva un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Evidentemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de los riesgos, considerando el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca.

Algunas medidas de seguridad que se pueden implantar en estos casos van desde el cifrado de información sensible para impedir su acceso sin la clave adecuada, métodos físicos de destrucción de la información en caso de manipulación mecánica de la misma, etc.

- **Fallos de seguridad en la utilización del software**

Se puede hacer un análisis agrupando los fallos de seguridad que se pueden dar en el software. Este análisis va a permitir enfocar, más adelante cómo distintos tipos de software ayudan a solventarlos. De una forma simplista, se pueden dividir en tres bloques:

  - Fallos debidos a errores desconocidos en el software, o conocidos sólo por terceras entidades hostiles.
  - Fallos debidos a errores conocidos pero no arreglados en la copia en uso del software.
  - Fallos debidos a una mala configuración del software, que introduce vulnerabilidades en el sistema.

El primero de ellos se puede achacar a la calidad del código, el segundo a la capacidad y celeridad de arreglo de los errores descubiertos en el código por parte del proveedor del mismo y a la capacidad del administrador de recibir e instalar nuevas copias de este software actualizado. El tercer tipo de vulnerabilidades puede achacarse, sin embargo, a una falta de documentación del software o una falta de formación adecuada de los administradores para hacer una adaptación correcta del mismo a sus necesidades.

Los fallos pueden dar lugar a un mal funcionamiento del programa, siendo en el ámbito de la seguridad bastante preocupantes por cuanto:

- Pueden implementarse algoritmos de forma incorrecta lo que puede llevar a una pérdida de seguridad (por ejemplo, un algoritmo de generación de claves que no se base en números totalmente aleatorios).

- Pueden diseñarse servicios que, en contra de sus especificaciones, ofrezcan funcionalidades no deseadas o que puedan vulnerar la seguridad del servidor que los ofrezca.

- Pueden no haberse tomado las medidas de precaución adecuadas para asegurar el correcto tratamiento de los parámetros de entrada, lo que puede hacer que un atacante externo abuse de ellos para obligar al programa a realizar operaciones indeseadas.

3.2.1 ¿Qué es el software libre? Para entender la situación de este tipo de software con respecto a su uso en seguridad informática es imprescindible describir, en primer lugar, a qué se refiere este documento cuando hace referencia a “software libre”[9].

[9] FERRER, Jorge y FERNÁNDEZ SANGUINO, Javier. Seguridad, informática y software libre [en línea] Hispalinux. Disponible en internet: http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf p. 7

El concepto de software libre es, en primera instancia, fácil de presentar, aun no existiendo una única descripción reconocida por todos de lo que es realmente este tipo de software. En general se entiende como software libre aquel programa o conjunto de ellos de los que el usuario puede disponer del código fuente, sin restricciones, y el cual puede modificar y redistribuir también sin restricciones. Estas libertades garantizadas al usuario del software (o a aquel que lo recibe) no son contrarias a los derechos legítimos del autor del programa, es decir, éste no tiene por qué perder sus derechos sobre el mismo. No se incluye, por tanto, en esta definición software en el "domino público" (aquél para en el que el autor ha cedido todos sus derechos).

Ventajas del software libre en el mundo de la seguridad. Si se analiza la descripción realizada previamente de la definición de software libre se derivan una serie de ventajas principales de este tipo de software sobre el software propietario, algunas de las cuales son muy adecuadas para el mundo de la seguridad. A saber:

Al disponer del código fuente de los programas en su totalidad, éste puede ser analizado por terceras personas ajenas a sus autores en busca de fallos de diseño o de implementación. Es decir, cualquiera con los conocimientos necesarios puede realizar una auditoría del código del programa.

- La posibilidad de realizar modificaciones libremente al código fuente y distribuirlas permite que cualquiera pueda ofrecer mejoras sobre éste. Estas mejoras podrán ser nuevas funcionalidades que se incorporen al mismo o parches que corrijan problemas detectados anteriormente.

- Las características del software libre hacen que no sea lógico cargar costes sobre el software en sí (dado que se ha de distribuir sin cargo), lo que permite que este tipo de software pueda ser utilizado por organizaciones y personas con menos recursos económicos. Esto se presenta como una ventaja cuando se compara con los precios de lo que cuesta el software de seguridad propietario hoy en día (licencias de cortafuegos, VPN, sistemas de detección de intrusos, etc.). El software libre pone en manos de cualquiera el tipo de tecnología que, hoy por hoy, sólo podían tener grandes corporaciones.

- De igual forma, la posibilidad de modificar libremente el software permite a las organizaciones que lo adapten a sus propias necesidades, pudiendo eliminar funcionalidades que no le sean de interés. En el mundo de la seguridad existe la máxima de "lo más sencillo es más seguro" por ello poder eliminar funciones innecesarias de las herramientas las puede convertir de forma inmediata en más seguras (porque no podrán ser utilizadas estas funcionalidades para subvertirlas). Frente al análisis de fallos que puede sobrevenir en la realización del software (presentado anteriormente), el software libre protege a sus usuarios con una serie de mecanismos determinados. Entre estos:

- La posibilidad de una auditoría de código en las herramientas software reduce los riesgos de seguridad debido a la aparición de fallos desconocidos, a la introducción de funcionalidades no deseadas en el código o la incorrecta implementación de algoritmos públicos. Aunque no se pueda asegurar que el código esté carente de errores, si es posible garantizar que tantas posibilidades tiene de encontrar un fallo de programación en éste (que lleve implícito un riesgo de seguridad) un atacante externo como la organización lo

utilice. Si bien no se puede asegurar que los mejores cerebros del mundo realicen la auditoría de código del software que una compañía utiliza, dicha compañía si tiene la posibilidad, en función de sus necesidades respecto a la seguridad, de realizar ella misma dicha auditoría de código o pagar a alguien para que la realice. Muchos de los proyectos de software libre, entre ellos el núcleo de Linux, el proyecto Apache, y la distribución OpenBSD realizan auditorías del código para asegurar su integridad, seguridad y ajuste a las especificaciones de funcionalidades requeridas.

- La posibilidad de corregir los programas y distribuir dichas correcciones permite que los programas evolucionen de una forma más abierta. En el mundo de la seguridad, un fallo en el sistema significa exponer a éste a una "ventana de vulnerabilidad" que tiene lugar desde la detección del fallo (por parte de sus usuarios legítimos o de terceras partes, hostiles incluso) a la aplicación de la medida correctiva, que pueda ser la instalación del parche adecuado que arregle el problema, pasando por la generación de dicho parche. El hecho de que la generación de dicho parche pueda realizarse por un número de personas (confiables) elevado, y no por un sólo fabricante, debe, en teoría, reducir este tiempo de exposición a dicha vulnerabilidad.

- El hecho de que exista una cierta independencia entre el software y su fabricante, o distribuidor original, permite que los usuarios de este software, en caso de pérdida de soporte, puedan realizar el mantenimiento de éste ellos mismos o subcontratarlo a una tercera empresa. Este hecho es, si cabe, de gran importancia en el mundo de la seguridad dado que la seguridad de una entidad no debe depender de la solvencia de terceras compañías a las que adquiere productos de seguridad y actualmente, sin embargo, es así. Debido a la gran variabilidad de riesgos potenciales contra los que un elemento de seguridad informática debe proteger, estos productos han de ser frecuentemente actualizados, muchas veces empujados por el descubrimiento de ataques antes desconocidos. Sin embargo, si una compañía depende de un producto de una tercera entidad y, de forma transitiva, de esta tercera entidad, la pérdida de soporte de este producto (por quiebra de la tercera entidad o abandono de una determinada línea de negocio) da lugar a que la compañía no esté adecuadamente asegurada contra los nuevos riesgos que puedan surgir. Las únicas opciones posibles serán mantener un sistema de seguridad que, con el tiempo, quedará obsoleto, o migrar a un sistema de seguridad nuevo (otro producto de otro fabricante) con sus consecuencias económicas y de impacto en servicios ya consolidados.

Las auditorías de código son, por tanto, posibles o no en determinados sistemas operativos en función de la publicidad dada a su código fuente. Sin embargo, no basta con decir qué se puede hacer una auditoría del código, es necesario considerar los resultados de dichas auditorías. Si bien Microsoft y Sun ofrecen el código fuente de su sistema operativo (el primero con más restricciones que el segundo), ninguno de los dos incorporará, necesariamente, los resultados de una auditoría de código sobre la base del sistema operativo realizado por terceras entidades. Los criterios para tomar dicha decisión no dependen de la auditoría en sí sino de la política de la propia compañía. Sin embargo, en la auditoría que se pueda realizar a sistemas operativos libres, como es el caso de GNU/Linux o BSD, la aplicación de los resultados o no se realiza mediante una discusión pública y es el propio resultado de la auditoría el que debe valer por si mismo para su introducción o no. No existen presiones comerciales de pérdida de imagen, ni el

"time to market" ni ningún tipo de consideraciones que no sean las puramente técnicas. Este mismo hecho, la modificación inmediata del código y su distribución, es el que puede dar lugar a que, aun cuando Sun distribuya de forma pública el código de Solaris, se audite de forma más intensiva el código de GNU/Linux o BSD, ya que son las propias personas que realizan la auditoría las que pueden sugerir implementaciones de las modificaciones sugeridas es que se podrán incorporarán rápidamente en el código auditado.

- **Desventajas del software propietario.** Sin embargo, el uso de software libre no está exento de desventajas. Así se podrían enumerar las siguientes:

    - La posibilidad de una generación más fácil de troyanos, dado que el código fuente también puede ser modificado con intenciones maliciosas. Si el troyano logra confundirse con la versión original puede haber problemas graves. La fuente del programa, en realidad, será el método de distribución de software, que, de no ser seguro, permitirá que un tercer agente lo manipule. La distribución de software se asegura añadiendo posibilidad de firmado de hashes de la información distribuida.

    - El método de generación de software libre suele seguir, en la mayoría de los casos, el modelo bazar, es decir, muchas personas trabajan sobre partes concretas e integrando sus cambios o personas desde el exterior contribuyen mejoras al proyecto global. Esto puede dar lugar a que se realice una mala gestión del código fuente del software por no seguir métodos formales de seguimiento, la consecuencia final es que falten piezas clave (que nadie ha contribuido) como es el caso de la documentación.
    - Al no tener un respaldo directo, la evolución futura de los componentes software no está asegurada o se hace demasiado despacio.

En mayor o menor medida, algunas de estas desventajas están comenzando a soluciones. El caso la difusión de troyanos se limita mediante el uso de técnicas de firma digital para garantizar la inviolabilidad del código o binarios transmitidos. Es frecuente que algunos autores de software libre al distribuir el código indique también información (sumas MD5 firmadas) que permitan garantizar la integridad del código descargado. Asimismo, las distribuciones del sistema operativo, como Debian o RedHat, han incorporado a lo largo del año 2001 soluciones de firma digital para la distribución de código fuente y binario de forma que el usuario pueda garantizar la integridad del mismo tras una descarga.

De igual forma, los problemas de evolución futura empiezan a quedar resueltos con un cambio de paradigma por parte de las compañías de software. Se trata del cambio de un modelo de negocio en el software que pasa a enfocar el negocio orientado al cobro de la realización de servicios en lugar del cobro a la utilización de productos. Ya se observan, en el mundo de software libre, compañías que contratan a personal cualificado para hacer mejoras sobre proyectos libres para cubrir sus propios intereses y ofrecen soporte de productos de software libre. Estas compañías, a diferencia de la orientación propietaria previamente presentada, siguen haciendo públicas las modificaciones realizadas al código fuente[10].

[10] Ibid. p. 7

3.3 VIRTUALIZACIÓN

"Es una opción simple para los departamentos de TI que desean implementar las herramientas más sofisticadas de administración y migración de máquinas virtuales. Es VMware".

3.3.1 ¿Qué es la virtualización? *"La virtualización es una tecnología probada de software que permite ejecutar múltiples sistemas operativos y aplicaciones simultáneamente en un mismo servidor. Está transformando el panorama de TI y modificando totalmente la manera en que las personas utilizan la tecnología"*[11].

Ventajas de la virtualización. La virtualización puede aumentar la escalabilidad, flexibilidad y agilidad de TI, al mismo tiempo que genera ahorros significantes en los costos. Las cargas de trabajo se implementan con mayor rapidez, el rendimiento y la disponibilidad aumentan, y las operaciones se automatizan. Todo esto hace que la administración de TI sea más simple y que la operación y la propiedad sean menos costosas.

- Reduzca los costos de capital y operacionales.
- Proporcione alta disponibilidad de las aplicaciones.
- Minimice o elimine el tiempo fuera de servicio.
- Aumente la capacidad de respuesta, la agilidad, la eficiencia y la productividad de TI.
- Acelere y simplifique el aprovisionamiento de recursos y aplicaciones.
- Respalde la continuidad del negocio y la recuperación ante desastres.
- Permita la administración centralizada.
- Desarrolle un verdadero centro de datos definido por el software[12]

3.3.2 Tipos de virtualización

- **Virtualización de servidores.** La mayoría de los servidores funcionan a menos del 15 % de su capacidad, lo que causa la expansión de servidores y aumenta la complejidad. Gracias a la virtualización de servidor, se abordan estas ineficacias mediante la ejecución de varios sistemas operativos en un único servidor físico como máquinas virtuales, y cada una de ellas tiene acceso a los recursos de procesamiento del servidor subyacente. Sin embargo, la virtualización de uno o dos servidores es solo el comienzo. El paso siguiente es agregar un clúster de servidores a un recurso único y consolidado, gracias a lo cual se aumenta la eficacia general y se reducen los costos. La virtualización de servidor también permite una implementación de cargas de trabajo más rápida, un aumento del rendimiento de las aplicaciones y una disponibilidad superior. Además, a medida que las operaciones se automatizan, la administración de TI se simplifica y la operación y propiedad se vuelven menos costosas. Para iniciar el camino hacia la virtualización de servidor, VMware ofrece vSphere with Operations Management. Permitirá virtualizar los recursos de servidores x86 y proporcionar características fundamentales para la administración de capacidad y rendimiento. Se diseñó para cualquier tamaño de empresa con el fin de ejecutar

[11] VM WARE INC. Virtualización [en línea] Disponible en internet: [Publicado Junio 30, 2016] http://www.vmware.com/co/virtualization/overview
[12] Ibid.

aplicaciones en niveles altos de servicio y maximizar los ahorros en hardware mediante una utilización de la capacidad incluso mayor e índices de consolidación aún más altos.

- **Virtualización de la red.** La virtualización de redes es la reproducción completa de una red física en software. Las aplicaciones se ejecutan en la red virtual exactamente del mismo modo en que lo hacen en una red física. La virtualización de red presenta dispositivos y servicios de red lógicos, es decir, puertos lógicos, switches, enrutadores, firewalls, equilibradores de carga, redes privadas virtuales (VPN, Virtual Private Network) y mucho más, para cargas de trabajo conectadas. Las redes virtuales ofrecen las mismas funciones y garantías que una red física, junto con las ventajas operacionales y la independencia de hardware propias de la virtualización. La plataforma de virtualización de NSX de VMware proporciona para las redes las capacidades que VMware ya suministra para el procesamiento y el almacenamiento. Al aplicar el modelo operativo de una máquina virtual a la red del centro de datos, puede transformar la economía de las operaciones de seguridad y red.

- **Almacenamiento definido por el software.** Los volúmenes grandes de datos y las aplicaciones en tiempo real están llevando las demandas de almacenamiento a nuevos niveles. Mediante la virtualización del almacenamiento, se separan los discos y las unidades flash en los servidores, se los combina en depósitos de almacenamiento de alto rendimiento y se los suministra como software. El almacenamiento definido por el software (SDS, Software-Defined Storage) es una nueva estrategia para el almacenamiento que brinda un modelo operacional fundamentalmente más eficaz. Como líder en almacenamiento definido por el software hiperconvergente para entornos virtuales, VMware Virtual SAN permite aplicar los principios del centro de datos definido por el software de VMware para el almacenamiento y ofrecer un aprovisionamiento simplificado basado en políticas. Se integra con vSphere Web Client, de modo que pueda administrar fácilmente el procesamiento y el almacenamiento mediante una única interfaz.

- **Virtualización de escritorios.** La implementación de escritorios como un servicio administrado le permite responder con mayor rapidez a las necesidades y las oportunidades cambiantes. Puede reducir costos y aumentar el servicio mediante el suministro rápido y sencillo de escritorios y aplicaciones virtualizados a las sucursales, a los empleados en el extranjero y tercerizados, y a los empleados móviles con tabletas iPad y Android. Las soluciones para escritorios de VMware, incluidos Horizon, Fusion y Mirage, son escalables, coherentes y completamente seguras, al mismo tiempo que poseen una alta disponibilidad, lo que permite garantizar un tiempo de servicio del sistema y una productividad óptimos.

- **¿Por qué las empresas deben virtualizar su infraestructura?** Virtualizar una infraestructura de TI permite reducir los costos de TI y aumentar la eficiencia, la utilización y la flexibilidad de los activos que posee. En todo el mundo, empresas de todos los tamaños aprovechan las ventajas de la virtualización con VMware. Miles de organizaciones, incluso todas aquellas que forman parte del ranking Fortune 100, utilizan las soluciones de virtualización de VMware. Conozca cómo la virtualización de toda su infraestructura de TI ayudará a su empresa[13].

[13] VM WARE INC. Tipos de Virtualización [en línea] Disponible en internet: http://www.vmware.com/co/virtualization/getting-started.html

3.3.3 Las 5 razones principales para adoptar un software de virtualización.

- **Obtener más ventajas con los recursos que posee:** agrupe recursos de infraestructura de uso habitual y rompa con el modelo tradicional de "una aplicación por servidor" mediante la consolidación de servidores.
- **Reducir los costos del centro de datos reduciendo la infraestructura física y mejorando el índice de servidores por administrador:** menos servidores y hardware de TI relacionado significan una reducción de espacio físico y de requisitos de energía y refrigeración. Las mejores herramientas de administración le permiten mejorar el índice de servidores por administrador, de manera que los requisitos de personar también se reducen.
- **Aumentar la disponibilidad de hardware y aplicaciones para lograr una mejor continuidad del negocio:** respaldar y migrar de manera segura entornos virtuales enteros sin interrumpir el servicio. Eliminar el tiempo fuera de servicio planificado y recupérese de inmediato de los problemas no planificados.
- **Ganar flexibilidad operacional:** responder a los cambios del mercado con una administración dinámica de recursos, un aprovisionamiento de servidores más rápido y una implementación mejorada del escritorio y las aplicaciones.
- **Mejorar la capacidad de administración y la seguridad del escritorio:** implementar, administrar y monitorear los entornos de escritorio seguros a los cuales pueden acceder los usuarios de manera local o remota, con o sin conexión de red, en casi todas las PC de escritorio, portátiles o tablets[14].

[14] PLCT S.A. de C.V. Virtualización [en línea] Disponible en internet: http://plct.com.mx/index.php/servicios/virtualizacion

4. INGENIERÍA DEL PROYECTO

4.1 RECURSOS

El éxito de la implementación de la solución, dentro de los tiempos estimados y satisfaciendo la necesidad planteada, requiere que se destinen una serie de recursos, económicos, humanos y de infraestructura, que se detallan a continuación.

4.1.1 Recursos económicos. Para la implementación exitosa de la solución, se debe contar con los siguientes recursos económicos Tecnología y Redes SAS ha dispuesto un total de $120.000.000, recursos que deberán ser suficientes y optimizados de la manera correcta para garantizar la entera satisfacción a la necesidad actual.

4.1.2 Recursos Humanos. También se requerirá como mínimo de grupo de tres personas, vitales para el cumplimiento de los objetivos propuestos, se detalla a continuación:

- Un (1) investigador e implementador, estudiante de ingeniería de sistemas en fase de terminación de materias.
- Un (1) director de proyecto, docente de la universidad y con capacidad de seguimiento y conocimientos detallados del tema para realizar los ajustes a los que haya lugar.
- Un (1) revisor de proyecto, docente de la universidad con conocimientos detallados en el ámbito de las tecnologías de información y las comunicaciones, con capacidad de realizar un chequeo de la documentación del proyecto.

4.1.3 Recursos Físicos. Son los medios necesarios para el desarrollo de la investigación, repositorios de información, insumos de papelería, tecnología y demás, detallados a continuación:

- Documentación digital y física; Libros, repositorios de información, video-tutoriales, comunidades virtuales interactivas y demás, con información pertinente para la implementación de la solución.
- Un (1) computador portátil con procesador Intel Core i5, 4GB de memoria RAM DDR3, licencia de sistema operativo Windows 7 Professional y superior, licencia de Microsoft Office 2010 Professional o superior y licencia de Microsft Visio Professional 2013 o superior.
- Una (1) impresora láser para impresión de documentación.
- Acceso a internet por ADSL o fibra óptica para consultar información publicada en la web pertinente al proyecto.

4.2 ANÁLISIS DE POLÍTICA DE SEGURIDAD ACTUAL, PROCESOS DE INFRAESTRUCTURA Y COMUNICACIONES

4.2.1 Política de seguridad, esquemas de protección perimetral y control de acceso. La compañía actualmente no cuenta con una política de seguridad bien estructurada, no cuenta con una política de control de acceso, back up y restauración, uso del software, gestión de activos de información, gestión de comunicaciones, gestión de uso de servicios de la red ni gestión de carpetas compartidas. La información se centraliza actualmente en una unidad de almacenamiento (arreglo de discos, RAID 5), en la cual se asignan permisos de autenticación por Directorio Activo, no obstante, no se han definido grupos de seguridad para asignación de privilegios según el rol de cada usuario. La seguridad perimetral el soportada con un appliance de firewall Dlink DFL 260, que cuenta con una sola interfaz WAN, lo cual hace imposible configurar un canal de datos de back up en modo o un servicio de balanceo de cargas.

4.2.2 Procesos de infraestructura, servicios base y comunicaciones. Todos los servicios de red básicos están concentrados en un servidor físico entran, con entorno Windows Server2008 R2, los roles configurados se detallan a continuación:

- Directorio Activo
- DHCP
- DNS
- Servidor de archivos
- FTP
- Servidor de impresión

Ninguno de estos servicios cuenta con replicación o contingencia, la instalación de actualizaciones se realiza en caliente y los reinicios requeridos para su aplicación se realizan en horas de la madrugada, cuando los niveles de transaccionalidad son bajos.

4.2.3 Distribución del centro de datos. La distribución actual del centro de datos se detalla a continuación:

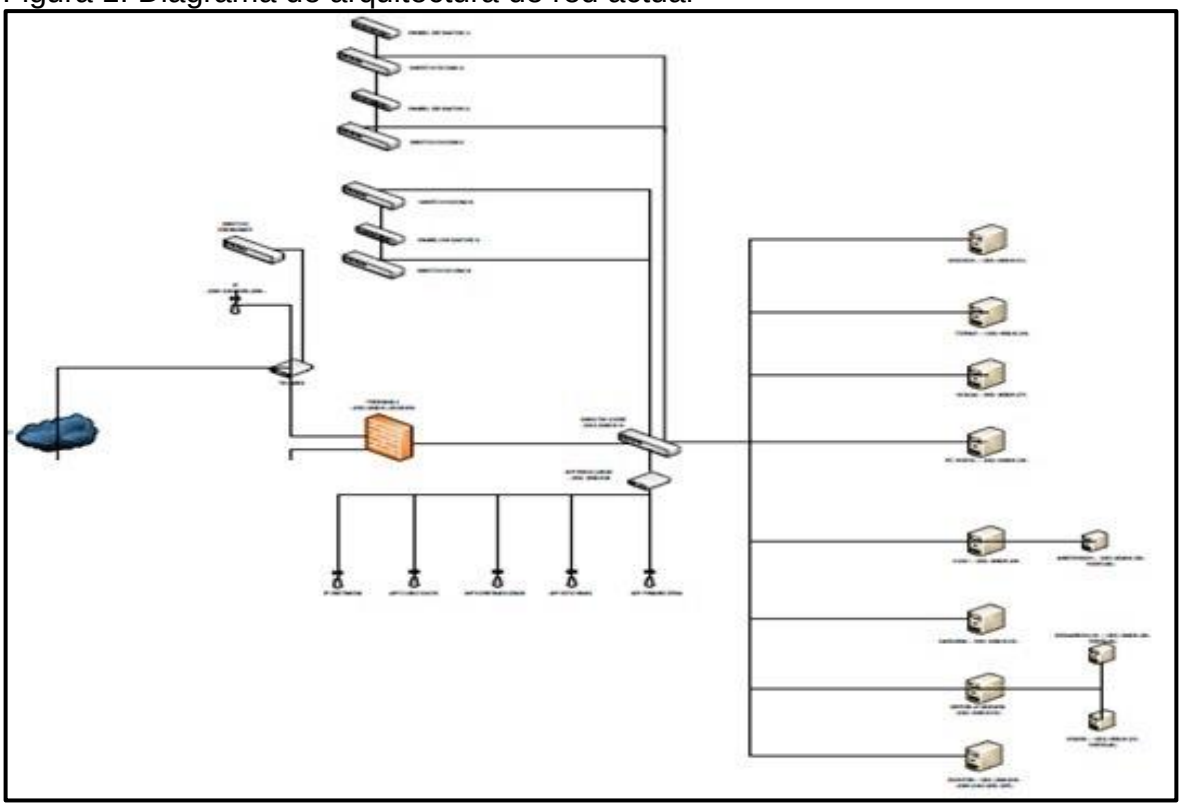
- 2 servidores de rack.
- 5 servidores de torre.
- 1 Firewall D-LINK DFL-210
- 1 Switch Core 3COM 4210 (Equipo principal y gateway de la red local).
- 5 Switch 3COM 4200.
- 1 Controladora de red inalámbrica HP PROCURVE MSM 710.
- 7 Access Point distribuidos en los dos pisos que reparten señal inalámbrica de internet.

- Planta telefónica Panasonic TDA 200 con 255 extensiones análogas y 48 extensiones digitales configuradas.

4.2.4 Distribución del centro de datos. La red de área local está distribuida en una topología de estrella, centralizada en un Switch Core 3COM 4210 y cinco Switch 3COM 4200 que distribuyen conectividad para 107 puntos de red instalados sobre cable UTP en categoría 6. Las comunicaciones inalámbricas son provistas con una controladora de red inalámbrica HP PROCURVE MSM 710 y 7 Access Point HP M220.

DIAGRAMA DE ARQUITECTURA ACTUAL CENTRO DE DATOS

Figura 1. Diagrama de arquitectura de red actual



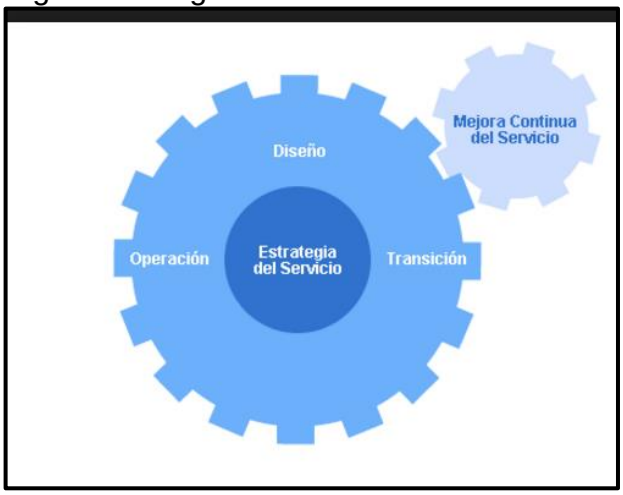
Fuente: Los Autores. La empresa

4.3 DEFINICIÓN DE ARQUITECTURA DE LA SOLUCIÓN

Siguiendo los estándares internacionales de buenas prácticas de IT (ITIL V3, TOGAF, COBIT), pensando en garantizar un proceso adecuando de transición de los servicios y cumpliendo a cabalidad cada uno de los pasos de su ciclo de vida, se plantea una arquitectura empresarial por ambientes, esto es, segmentos de red aislados por firewall de borde, cada uno independiente de los otros y cada uno cumpliendo con funciones propias de estándares de calidad.

CICLO DE VIDA DEL SERVICIO

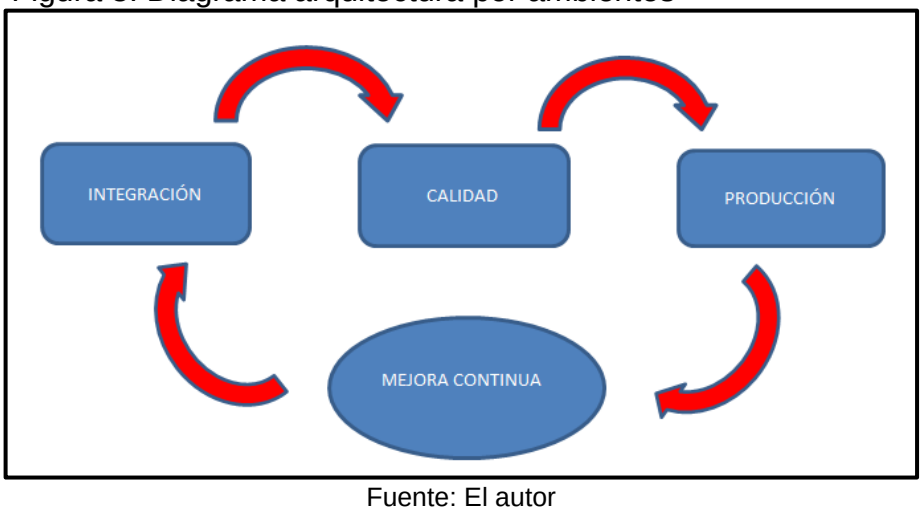
Figura 2. Diagrama de ciclo de vida del servicio



Fuente: El autor

ARQUITECTURA POR AMBIENTES

Figura 3. Diagrama arquitectura por ambientes



Fuente: El autor

4.3.1 Ambiente de integración: Ambiente utilizado por el diseñador del servicio para realizar pruebas integrales de éste, estas pruebas deberán garantizar que se cumpla a cabalidad con las especificaciones determinadas previamente y que la integración con otros sistemas, la funcionalidad modular y el alcance del servicio sean cubiertos de manera adecuada. El administrador del servicio deberá certificar todo lo anterior para poder continuar con el siguiente paso del ciclo de vida del servicio.

4.3.2 Ambiente de calidad: Ambiente utilizado por el usuario final del servicio para realizar pruebas funcionales de éste, el usuario final deberá verificar que se cumpla con las especificaciones planteadas desde el inicio por el área de negocio. El aseguramiento de la calidad permitirá a la compañía un importante ahorro a futuro, corrigiendo posibles fallas en los servicios antes de que éstos se encuentren productivos. Es requisito que el usuario funcional certifique que todo lo anterior se cumpla a cabalidad para poder continuar con el siguiente paso del ciclo de vida del servicio.

4.3.3 Ambiente de producción: Es el núcleo del negocio, los servicios en producción ya han sido depurados y corregidas sus posibles fallas. No obstante, todos los servicios productivos están sujetos a un proceso de mejora continua, y el rol encargado de autorizar el paso de servicios a producción, según lo indica la fase de transición del servicio de ITIL V3, será el comité de cambios de la compañía.

4.4 DEFINICIÓN DE UNA TOPOLOGÍA DE RED SEGURA

Para el diseño de un esquema de red adecuado, se tuvo en cuenta el crecimiento exponencial de la infraestructura de la organización, la demanda creciente de servicios en producción, la diversificación constante del mercado y el incremento latente de clientes de la organización.

Se define un direccionamiento clase A, con una capacidad de alojamiento de 406 host por ambiente, se detalla a continuación.

Tabla 1. Diagrama arquitectura de red ambiente de producción

DIRECCIONAMIENTO CDP AMBIENTE DE PRODUCCION							
VIRTUAL SYSTEM	ZONA	SERVICIOS	IP	MASCARA	Host	VLAN	GATEWAY
INTERNET	DMZ 1	Servicios Web	10.100.50.128	28	14	1052	10.100.50.129
BACKEND	SERVICIOS DE RED	DHCP, DNS, DA	10.100.60.0	27	30	1053	10.100.60.1
	FILESERVER	FTP Inteno/Externo Servidores de Impresión	10.100.60.30	27	30	1054	10.100.60.31
	APLICACIONES	Servidores de Aplicación Exter	10.100.70.0	27	30	1055	10.100.70.1
	Bases de Datos	Sybase, Oracle, SQL	10.100.73.0	27	30	1056	10.100.73.1
	ESTACIONES DE TRABAJO	estaciones de trabajo	10.100.80.0	24	254	1057	10.100.80.1
TERCEROS	QBE SEGUROS	Conexión QBE Seguros	10.200.50.8	28	14	1058	10.100.50.9

Fuente: El autor

Tabla 2. Diagrama arquitectura de red ambiente de calidad

DIRECCIONAMIENTO CDP AMBIENTE DE CALIDAD							
VIRTUAL SYSTEM	ZONA	SERVICIOS	IP	MASCARA	Host	VLAN	GATEWAY
INTERNET	DMZ 1	Servicios Web	10.120.50.128	28	14	1052	10.120.50.129
BACKEND	SERVICIOS DE RED	DHCP, DNS, DA	10.120.60.0	27	30	1053	10.120.60.1
	FILESERVER	FTP Inteno/Externo Servidores de Impresión	10.120.60.30	27	30	1054	10.120.60.31
	APLICACIONES	Servidores de Aplicación Exter	10.120.70.0	27	30	1055	10.120.70.1
	Bases de Datos	Sybase, Oracle, SQL	10.120.73.0	27	30	1056	10.120.73.1

Fuente: El autor

Tabla 3. Diagrama arquitectura de red ambiente de integración

DIRECCIONAMIENTO CDP AMBIENTE DE INTEGRACIÓN							
VIRTUAL SYSTEM	ZONA	SERVICIOS	IP	MASCARA	Host	VLAN	GATEWAY
INTERNET	DMZ1	Servicios Web	10.130.50.128	28	14	1052	10.130.50.129
BACKEND	SERVICIOS DE RED	DHCP, DNS, DA	10.130.60.0	27	30	1053	10.130.60.1
	FILESERVER	FTP Inteno/Externo Servidores de Impresión	10.130.60.30	27	30	1054	10.130.60.31
	APLICACIONES	Servidores de Aplicación Exter	10.130.70.0	27	30	1055	10.130.70.1
	Bases de Datos	Sybase, Oracle, SQL	10.130.73.0	27	30	1056	10.130.73.1

Fuente: El autor

4.5 DEFINICIÓN DE POLÍTICA DE SEGURIDAD

El diseño e implementación de una política de seguridad acorde con los estándares internacionales de buenas prácticas de IT, permitirá a la organización mitigar riesgos y prevenir amenazas a los sistemas de información, mediante directrices que orienten sobre el correcto uso de los servicios tecnológicos de la compañía y recomendaciones para obtener un mayor beneficio de ellos y evitar su uso inadecuado.

Partiendo desde un análisis de los riesgos existentes, la política de seguridad surge como una herramienta que permitirá sensibilizar al personal en general de la compañía acerca de la importancia de garantizar la disponibilidad, confidencialidad e integridad de la información, siendo está el núcleo vital de cualquier negocio, y siempre enmarcada dentro de la mejora continua, lo cual asegura la competitividad de la organización.

La política de seguridad se compone de una seria de procedimientos detallados a continuación:

4.5.1 Política de correo electrónico

- **Objetivo.** Dictar las directrices y lineamientos para el uso del correo electrónico corporativo para el desempeño de sus funciones dentro de la organización.

- **Alcance.** La presente política aplica a todos los procesos de la entidad, a todos sus servidores y colaboradores de Tecnología y Redes SAS, así como contratistas y personal externo o temporal que esté autorizado para hacer uso del correo corporativo.

- **Tipos de cuentas de correo.** Todas las cuentas de correo que existen en Tecnología y Redes SAS son propiedad de la entidad y se clasifican de la siguiente manera:

    - **Cuentas individuales:** Los servidores y colaboradores de **Tecnología y Redes SAS** tendrán una cuenta de correo para el uso diario de sus actividades laborales. El nombre de dicha cuenta se ajustará al formato inicialnombreapellido@tcnoredes.net.co, que variara según las circunstancias que eviten la duplicidad en su conformación.
    - **Cuentas Grupales**: Estas cuentas son creadas para las necesidades de comunicación Interna de la entidad entorno a la gestión de áreas específicas. Deben ser solicitadas directamente por el líder de grupo o área interesada. El nombre de la cuenta de correo se conformará en el formato nombredepartamento@tcnoredes.net.co, El titular del área será responsable del uso que se dé a dicha cuenta.

Restricciones y prohibiciones. Están completamente prohibidas las siguientes actividades:

- Utilizar el correo electrónico para propósitos personales, económicos o comerciales ajenos a las actividades propias del cargo y de **Tecnología y Redes SAS**.
- Participar en la propagación de mensajes en “cadenas”, o esquemas piramidales dentro y fuera de la **Tecnología y Redes SAS**.
- Distribuir de forma masiva mensajes con contenidos que desborden el ámbito de competencias de la Empresa o que pongan en riesgo la operación de la entidad.
- Divulgar mensajes con datos o información institucional no autorizada.
- Enviar o reenviar mensajes con contenido difamatorio, ofensivo, irrespetuoso, racista u obsceno.
- Copiar o reenviar mensajes sin la autorización del remitente original.
- Enviar mensajes anónimos, así como aquellos que consignen seudónimos, títulos, cargos o funciones no oficiales.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Enviar correos SPAM de cualquier índole. Se consideran correos SPAM aquellos enviados de forma masiva no relacionados con las funcione específicas y generales del cargo y con los procesos y misión general de **Tecnología y Redes SAS**
- Utilizar el correo electrónico de otro funcionario sin su consentimiento, para él envió o recepción de mensajes e información.
- Enviar por correo electrónico a personas o entidades ajenas a **Tecnología y Redes SAS**, información de carácter interna o confidencial sin la debida autorización expresa de su superior inmediato.

4.5.2 Política de control de acceso

Objetivo. Controlar el acceso a la información de **Tecnología y Redes SAS**, de forma segura.

Alcance. La siguiente política aplica a:

- Todo tipo de acceso lógico a los activos de información que hacen parte de los sistemas de información de **Tecnología y Redes SAS**.

- Se hace referencia al acceso lógico de los activos de información de los sistemas de información cuando se autoriza el acceso a:
  - Las bases de datos
  - La documentación
  - Los programas y servicios prestados
  - La administración
  - Las redes y el sistema operativo
  - Todos los usuarios internos y externos de **Tecnología y Redes SAS**. que se encuentran autorizados para acceder a los sistemas de información y cualquiera de sus aplicaciones.

Responsabilidades de los propietarios de los activos de información. Los propietarios de los activos de información son los responsables de:

- Identificar toda la información que corresponda a su área de responsabilidad dentro de los sistemas de información cualquiera que sea su forma y medio de conservación.
- Clasificar toda la información de su propiedad de acuerdo con el grado de criticidad de los mismos y mantener un registro actualizado de la información más sensible.
- Autorizar el acceso a la información de los sistemas de información al personal interno de Tecnología y Redes SAS. y terceros (proveedores y contratistas) de acuerdo con sus respectivas funciones.
- Autorizar cualquier transmisión, envío, impresión y destrucción de información sensible que comprometa los sistemas de información.
- Definir los eventos de seguridad que considere necesario para la protección de la información.

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - Definir los eventos y actividades de usuarios a ser registrados en los sistemas de información y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales.

- Revisar en forma periódica las autorizaciones de acceso para asegurar que éstas sean aún válidas.

Requerimientos para el control de acceso. Todas las áreas responsables de aplicar controles de acceso deberán tener en cuenta los siguientes aspectos al momento de aplicar los controles de acceso sobre las aplicaciones:

- Identificar los requerimientos de seguridad para los sistemas de información y sus aplicaciones.
- Crear los perfiles de acceso a los sistemas de información y a los datos acorde con los roles y responsabilidades del personal.
- Identificar la legislación aplicable y obligaciones contractuales con respecto a la protección del acceso a datos y servicios de información que hacen parte de los sistemas de información.
- Definir perfiles de acceso de usuarios estándar, especiales y administradores, comunes a cada categoría de cargos y funcionarios que hacen parte de los sistemas de información.
- Administrar y controlar los derechos de acceso a los sistemas de información en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

Reglas de control de acceso. Las medidas de control de acceso para los sistemas de información especificadas, deberán contener los siguientes aspectos como mínimo:

- **Autorización de acceso a los sistemas de información:** Todas las áreas responsables de aplicar controles de acceso deberán aplicar el procedimiento formal de autorización que permite a los usuarios (internos y externos) el acceso a los sistemas de información. La autorización es dada por parte del propietario de la información, una vez el usuario haya hecho la solicitud mediante los formatos o mecanismos definidos para tal fin. Luego de su aprobación, ésta es radicada en la herramienta de gestión de incidentes y requerimientos (GLPI), quienes tramitarán su solicitud a través de los administradores de los sistemas de información.

- **Administración de acceso de usuarios a los sistemas de información:** Todas las áreas responsables de la administración de los sistemas de información deberán hacer uso de los procedimientos formales para controlar la asignación de derechos de acceso. Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de usuario como el registro de usuarios, la administración de privilegios, administración de contraseñas y revisión de derechos de acceso.
- **Control de acceso a la red que utilizan los sistemas de información:** El área de IT controla el acceso a los servicios de red que se relacionan con los sistemas de información tanto internos como externos. Esto es necesario para

garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios que hacen parte de los sistemas de información. Se tiene en cuenta la utilización de los servicios de red, la autenticación de usuarios para conexión externa, la utilización de los servicios de red, la protección de los puertos de diagnóstico remoto, las segmentaciones que se realicen a la red, el control de conexión a la red y el control de ruta en la red.

- **Monitoreo y uso de los sistemas de información:** Los sistemas de información core del negocio y las que se consideren necesarias podrán ser monitoreados con el fin de:

  - Detectar desviaciones
  - Registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad.
  - Generar registros de auditoría que contengan excepciones y otros eventos relativos a seguridad. Estos se mantienen durante un período definido para acceder en futuras investigaciones y en el monitoreo de control de acceso.
  - Establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información. Dichos procedimientos son necesarios para garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente.
  - Establecer un nivel de monitoreo requerido para cada una las instalaciones donde se encuentran ubicados los sistemas de información. Se determina mediante una evaluación de riesgo.
  - Revisar periódicamente el resultado de las actividades de monitoreo. La frecuencia de la revisión depende de los riesgos involucrados.

4.5.3 Política de backup y restauración

Generalidades. El back-up refiere a la copia o respaldo periódico de los datos e información a algún dispositivo de soporte de almacenamiento, desde el cual posteriormente podrán ser restaurados en caso de que un incidente ocasione la pérdida o corrupción de los datos originales, contribuyendo a asegurar la disponibilidad e integridad de la información y de los sistemas que lo soportan.

Los lineamientos y procedimientos de restauración de información son parte importante de la estrategia de seguridad para asegurar que las aplicaciones y su información pueden ser recuperadas tras un error o incidente.

Política. Los contenidos del proceso de respaldo de información o back-up deben determinarse considerando las necesidades de **Tecnología y Redes SAS**, sus aplicaciones y la criticidad de la información, acorde con los criterios identificados en la matriz de activos de información por proceso. El tipo de back-up realizado

debe reflejar la criticidad de los contenidos y la necesidad de garantizar la continuidad de las operaciones de negocio.

Tipos de Back-up. Deben realizarse, almacenarse y posteriormente sobrescribirse back-ups completos en un ciclo rotativo con un mínimo de tres generaciones de copias; estos ciclos de backup incluyen la retención cíclica para satisfacer necesidades no previstas de negocio, auditoría o forenses.

- **Back-up Completo:** Una copia completa de todos los datos de un sistema o dispositivo para servir como línea de partida.
- **Back-up Diferencial:** Una copia de todos los datos que hayan cambiado desde el último backup completo.
- **Back-up Incremental:** Una copia de todos los datos que hayan cambiado desde el último backup realizado.

Métodos. Pueden ser utilizados para la realización de los back-ups dos métodos:

- **Por servidor:** en este caso el backup se realiza sobre la totalidad de un disco o servidor sin considerar las características particulares de los diferentes contenidos que alojen. Los requisitos específicos de estos backup serán definidos por los propietarios de los servidores, que considerarán los requerimientos de seguridad asociados a la información más crítica y sensible entre la totalidad de contenidos del backup.

- **Por contenidos:** en este caso se realiza una selección de contenidos de backup de acuerdo a las necesidades concretas de negocio o legales de las diferentes áreas o unidades.

Las copias de back-up deben llevar asociada una información descriptiva que facilite la posterior restauración.

Ciclos de Backup. La frecuencia de realización de los Back-up debe estar determinada por las necesidades de negocio y los requerimientos normativos, legales y reglamentarios, tomando como base, las Tablas de Retención Documental de la entidad, el Análisis de Impacto del Negocio (BIA) que determina la criticidad de los procesos, por su información y disponibilidad.

Los sistemas de producción de uso diario, que hacen uso de información de los clientes de **Tecnología y Redes SAS**. y que realizan cualquier tipo de operación relacionada con el objeto y ser de la entidad, deben realizar back-up diario y completo.

Los ciclos de back-up incluirán copias periódicas para retención (semanales, mensuales, trimestrales y/o anuales) que deberán ser administrados y

determinados por el área de IT, para satisfacer los requisitos del negocio, de auditoría, continuidad o regulatorios.

Almacenamiento del backup. El almacenamiento de las copias de seguridad, debe realizarse en un lugar seguro dotado de medidas de control de acceso físico, acorde con la criticidad de los contenidos. (Armarios con cierre, controles de acceso, guardias de seguridad, etc.)

Los lugares de almacenamiento de las copias de respaldo deben presentar bajo nivel de riesgo de incendio, inundación, contaminación química o electromagnética. De igual manera las condiciones de humedad y temperatura se deben controlar acorde con las especificaciones del fabricante. Sólo personal autorizado del área de IT, podrá acceder y manipular los medios de soporte y respaldo de información.

Si las copias de almacenamiento son resguardadas por un tercero, debe mantenerse registro y soporte cuando éstas salgan y entren de la organización o su centro de datos, y se debe garantizar que son localizables y se pueden recuperar de forma ágil en caso de un incidente.

Eliminación de los medios de copia. Los soportes de almacenamiento de información deben ser eliminados de forma segura al final de su vida útil o al alcanzarse el número máximo de usos recomendado por el fabricante. Para tal efecto debe realizar la destrucción de los medios de forma física, o el borrado seguro, para garantizar que no se divulga la información allí contenida.

En el evento que se active el proceso de destrucción y/o eliminación de los medios de almacenamiento, se deberá dejar registro de dicha actividad, mediante un acta.

4.5.4 Política de gestión de activos de información

Objetivo. Asegurar que cada activo de información tenga un propietario y que la naturaleza y el valor de cada activo se maximice mediante una adecuada gestión durante todas las etapas de su ciclo de vida, desde el momento en que se crea o recibe, a través de su procesamiento, comunicación, uso y transporte, el almacenamiento y/o disposición. También asegura que los límites de uso aceptable estén claramente definidos para cualquiera que tenga acceso a la información, y que se protejan acorde con la criticidad que tengan para Tecnología y Redes SAS.

Alcance. Esta política aplica a todos los procesos de Tecnología y Redes SAS, desde la identificación del Propietario del activo valoración de riesgos y clasificación de la información. Se consideran activos de información los siguientes:

- Hardware.
- Software.
- Servicios
- Personas.
- Información. (Física o Digital)

Todo activo de información de **Tecnología y Redes SAS** es de uso exclusivo de la Entidad y será utilizado únicamente para su propósito especificado.

Tecnología y Redes SAS mantendrá un inventario actualizado de los activos de información existentes, con su correspondiente clasificación y propietario.

Inventario de activos de información. Cada líder de área identificará, clasificará y mantendrá registro documentado de los activos de información de sus procesos, acorde con los lineamientos y acompañamiento del área de Gobierno de Información. El inventario de activos de información incluirá: nombre, descripción, propietario, custodio, tipo de activo, atributos, valor, clasificación, acceso y ubicación. El inventario de activos de información será actualizado cada vez que el proceso identifique un nuevo activo o deba retirarlo.

Uso aceptable de la información. Todos los funcionarios, terceros (proveedores y contratistas) tendrán que cumplir las siguientes reglas para el uso de los activos de información:

- Todo funcionario que tenga acceso a cualquiera de los activos de información de **Tecnología y Redes SAS**, deberá utilizarlos solo para labores relacionadas con sus funciones, procedimientos en los que participa, servicios que presta o responsabilidades asignadas.

- Todo funcionario es responsable del uso adecuado de los recursos o activos de información bajo su responsabilidad, en el desarrollo de sus funciones, por lo que debe garantizar, que su acceso, divulgación, disponibilidad e integridad sean conservadas, bajo las reglas y condiciones de las actividades definidas en su proceso.

Clasificación de la información. Los activos de Información de Tecnología y Redes SAS serán clasificados para definir un conjunto apropiado de niveles de protección. Para tal efecto la clasificación y etiquetado de la información se debe hacer de acuerdo a los riesgos que existan en la divulgación de la información. Se debe etiquetar la información cuando esta se considere de carácter confidencial o privado, para lo cual se deberá hacer uso de marcas de agua, o títulos informativos en los sobres, documentos, informes, cartas u otras comunicaciones e información que indiquen su clasificación. La información una vez clasificada

puede ser reclasificada con base en criterios objetivos del propietario de ésta, conforme a los procedimientos establecidos para el efecto.

Categorías de clasificación de la información. Las categorías de clasificación de la información son definidas teniendo en cuenta los principios de la seguridad de información (Confidencialidad, Integridad y Disponibilidad) y los principios de calidad de la información (Exactitud, Completitud, Consistencia y Trazabilidad). Toda la información de Tecnología y Redes SAS es clasificada en los siguientes niveles:

- **Información pública.** Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que esto implique daños a terceros ni a las actividades y procesos de Tecnología y Redes SAS.

- **Información Interna:** Es la información que los funcionarios deben conocer para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo.

- **Información Restringida:** Información que es utilizada por un grupo reducido de personas y que no debe ser de conocimiento para otros funcionarios o terceros sin autorización del propietario del activo, ya que su publicación o divulgación no autorizada podría generar impactos negativos a la entidad.

- **Información Confidencial o Sensible:** Información cuya divulgación no autoriza supone un riesgo para el negocio y puede afectar la integridad de Tecnología y Redes SAS, su buena imagen o incumplir gravemente requisitos regulatorios o contractuales. Está restringido solo a personal expresamente autorizadas por el propietario. Se considera información sensible toda aquella que afecta la intimidad de las personas cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Se considera confidencial para efectos de lo aplicado aquí, toda aquella información que contenga, información de tipo identificación personal, como numero de cedula, información monetaria de cualquier tipo, créditos, saldos, cupos y movimientos, siempre que vayan acompañados del nombre o número de identificación del cliente. Igualmente, se considera confidencial, toda información que puede presentar riesgos importantes para Tecnología y Redes SAS, de tipo operativo, legal, regulatorio, reputacional, de seguridad o económico y por lo cual se deben contemplar medidas adicionales de control, procesos de autorización, conservación, transporte, divulgación a terceros, oportunidad de utilización y

destrucción, y cuyo acceso tiene que ser autorizado por el propietario de la información o su delegado y restringido a un grupo reducido de usuarios que la requiera para el uso de sus labores.

4.5.5 Política de gestión de comunicaciones y operaciones

Objetivo. Garantizar el funcionamiento correcto y seguro de la operación de los servicios de información, minimizando los posibles daños en las operaciones de los sistemas que se encuentran en producción, y en efecto, preservar la seguridad de la información.

Alcance. Desde las instalaciones de procesamiento y transmisión de información de Tecnología y Redes SAS hasta el mantenimiento constante de los activos de información (software, hardware, políticas, procedimientos, procesos, instructivos, personas e información).

Política. Se debe asegurar el funcionamiento correcto y seguro de los recursos para el tratamiento de la información y establecer las responsabilidades y procedimientos para la gestión y operación de los recursos de información. Tecnología y Redes SAS debe proteger la infraestructura, física y lógica de comunicaciones, así como sus sistemas de información con el fin de comprobar que no se pone en peligro la integridad, confidencialidad y disponibilidad de los activos de información.

Separación de los entornos de Integración, calidad y producción.
Deben existir como mínimo tres ambientes de operación en los sistemas de informaciónn de **Tecnología y Redes SAS**, uno de integración, otro de calidad y otro de producción, para reducir el riesgo de cambios en tecnologías de Información o de accesos no autorizados a los sistemas de información de **Tecnología y Redes SAS**.

Los siguientes controles deben ser considerados:

- Definir y documentar los procedimientos para la transferencia de software desde desarrollo al estado de pruebas y de éste, al estado de producción. Tales transferencias deben requerir la aprobación del propietario de la información y del área de IT de **Tecnología y Redes SAS**.
- El software en desarrollo y en producción debe ejecutarse en diferentes ambientes.
- Las actividades de desarrollo y prueba deben realizarse por separado.
- Cuando no es requerido, los compiladores, editores y otros utilitarios del sistema no deben ser accesibles desde los diferentes ambientes que estén en producción.

4.5.6 Política de uso de servicios de la red

Objetivo. Asegurar la protección de la información en las redes de Tecnología y Redes SAS. (Tanto alámbricas como inalámbricas – se extiende a la transmisión de datos por el aire en un entorno normalmente limitado a una oficina o edificio) y la protección de la infraestructura de soporte a través de un conjunto de requerimientos generales.

Alcance. La presente política aplica a todas las redes de Tecnología y Redes SAS, administradas y controladas por el área de IT, sobre la cual recae la responsabilidad de implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. La presente política está dirigida a los responsables de diseñar, operar o mantener estas redes así como aquellos que pudieran solicitar la conexión a las mismas.

Consideraciones de seguridad. A continuación se definen los requerimientos de seguridad que deben estar presentes en Tecnología y Redes SAS para garantizar que la red está correctamente configurada:

- La red estará disponible y correctamente dimensionada acorde a las necesidades de **Tecnología y Redes SAS**.
- Debe existir y mantenerse un mapa de red actualizado que contenga un mínimo de información de los siguientes entornos (conexiones con terceros, DMZ, conexión a redes WAN) además tiene que incluir información de los elementos de control de acceso que pudieran existir.
- La red de **Tecnología y Redes SAS**. será objeto de monitoreo para garantizar su disponibilidad, rendimiento y facilitar la gestión de incidentes.
- Las sesiones inactivas deben cerrarse después de un período determinado de inactividad en los servidores.
- Los dispositivos de red necesarios contarán con el respaldo adecuado, permitiendo restaurar las configuraciones de dichos dispositivos cuando se requiera.
- Las medidas de alta disponibilidad deben adaptarse y aplicarse a la tipología de datos transmitidos por la red.
- La red de **Tecnología y Redes SAS**. debe estar correctamente segmentada y protegida con dispositivos adicionales cuando lo requiera su exposición a riesgos (p. ej.: Internet, conexión con terceros, movilidad).
- Deben existir entornos de integración, calidad y producción en todas las arquitecturas de red. Esto formará parte del proceso de implementación de una arquitectura de red.
- Cualquier conexión con redes externas a **Tecnología y Redes SAS**., debe ser autorizada y contar con las medidas de seguridad adecuadas para el cumplimiento de requerimientos de la evaluación de riesgos.

- Cualquier conexión con redes externas debe ser autorizada y contar con las medidas de seguridad adecuadas para el cumplimiento de requerimientos regulatorios y de solución de riesgos.
- Los servicios visibles entre diferentes redes deben estar restringidos para permitir sólo el acceso a los servicios requeridos.
- No se permite la visibilidad entre dos redes que no sea necesaria, evitando así la propagación de problemas de unas redes a otras.
- Los sistemas de información que provean servicios a los usuarios deben estar ubicados en redes específicas de servidores, separadas de las redes de usuarios.
- Debe prohibirse la conexión de dispositivos que incumplan las medidas de seguridad definidas, puenteando zonas de distinto nivel de confianza, tales como interconexión directa entre diferentes redes.
- La conexión de nuevos dispositivos a la red de **Tecnología y Redes SAS**, se debe solicitar formalmente con anterioridad a la Gerencia Nacional de Infraestructura, quien evaluará el impacto y presentará el cambio a producción en el Comité de Cambios de la entidad.
- Los sistemas y dispositivos de comunicaciones conectados a la red deben estar correctamente bastionados (fortificar o reforzar las defensas frente a potenciales atacantes) para evitar la posibilidad de que se pueda explotar vulnerabilidades que pueda afectar a la seguridad, disponibilidad o rendimiento de la red.
- Se debe aplicar el registro y el monitoreo adecuado para permitir el registro de acciones de seguridad pertinentes
- En cualquier acuerdo sobre los servicios de red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si éstos se prestan al interior de **Tecnología y Redes SAS** o se contratan externamente.

4.5.7 Política de licenciamiento y uso del software

Objetivo. Garantizar la aplicación de los procedimientos para el licenciamiento y uso de software. Teniendo en cuenta los derechos de autor, el cumplimiento de las leyes y regulaciones asociadas con software. Así mismo, contar con las debidas autorizaciones para instalar software en los equipos de cómputo de Tecnología y Redes SAS, mantener en custodia las licencias adquiridas, recibidas en servicio por Tecnología y Redes SAS y realizar verificación periódica del software instalado.

Alcance. La presente política de licenciamiento y uso de software en Tecnología y Redes SAS, se aplica a todos los procesos de adquisición, desarrollo, uso, mantenimiento, terminación del ciclo de vida y renovación de cualquier tipo de software instalado o proyectado para usar en Tecnología y Redes SAS.

La política debe ser atendida por todos los usuarios de equipos de cómputo - incluyendo pero no limitándose a tabletas, portátiles, computadores de escritorio y servidores; que hayan sido adquiridos por **Tecnología y Redes SAS**, que estén a disposición de **Tecnología y Redes SAS** a través de un contrato de servicios o que sean utilizados para actividades propias de la entidad, de tal forma que se utilice software que garantice el cumplimiento de los requerimientos y la conformidad legal nacional e internacional, en especial la protección de la propiedad intelectual y los derechos de autor.

Además, incluye la conciliación del software actual instalado con la base de datos de registros de licencias adquiridas y desplegadas y la revisión periódica de la existencia de cualquier software en violación o superiores a las licencias adquiridas.

Lineamientos. El software de computador (incluyendo el manual de usuario y cualquier otra documentación que lo acompañe) está protegido por leyes que prohíben el uso y copia no autorizados.

Si un servidor de **Tecnología y Redes SAS** viola los derechos de autor al hacer o usar copias no autorizadas de software, podrá ocasionar consecuencias legales tanto a él mismo como a la organización, lo cual recae en un riesgo legal.

Uso del software. Un usuario no debe instalar software en los equipos de cómputo de Tecnología y Redes SAS por su propia cuenta, dicha función debe ser solicitada por el usuario a través de la mesa de servicio y coordinada con los funcionarios del área de IT quienes verificarán el licenciamiento disponible.

Sin importar el tipo de software, se debe solicitar al fabricante del software una aclaración por escrito sobre el tipo y uso del software, o contar con la evidencia de un sitio de soporte público y oficial, como las páginas de preguntas frecuentes que el fabricante publique en su sitio web oficial.

Responsabilidad del usuario. Un usuario de software debe usar el mismo con estricto apego a los términos y condiciones del Acuerdo de Licenciamiento. Un usuario de software no debe correr riesgos confiando en su interpretación del Acuerdo de Licenciamiento para determinar si un uso o copia en particular está permitido.

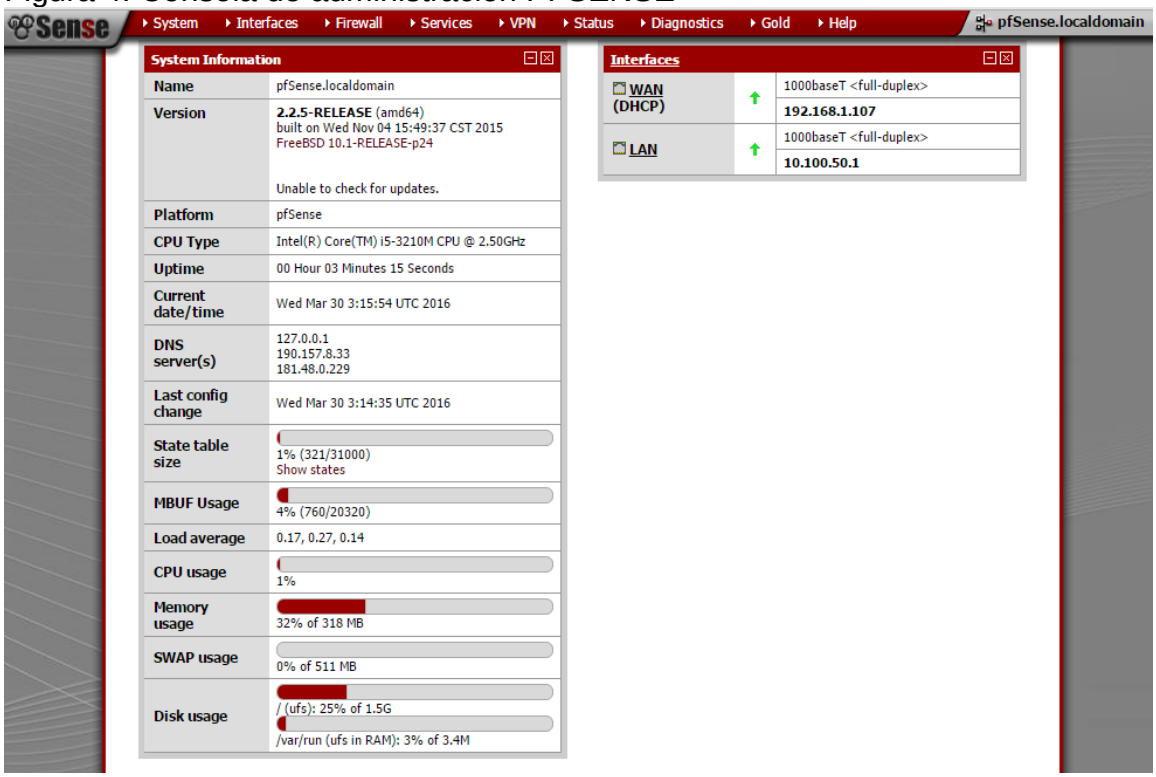
5. IMPLEMENTACIÓN DE SOLUCIONES DE SEGURIDAD Y VIRTUALIZACIÓN

5.1 INSTALACIÓN DE FIREWALL PERIMETRAL PFSENSE

Se procede a realizar la instalación de la solución perimetral de seguridad PFSENSE, solución que soportará todas las configuraciones de red, comunicaciones y seguridad de borde y perimetral necesarias para una operación óptima.

La siguiente gráfica muestra la configuración inicial de la solución, antes de realizar la creación e interfaces y asignación de redes virtuales (Vlan) según la topología de red definida anteriormente:

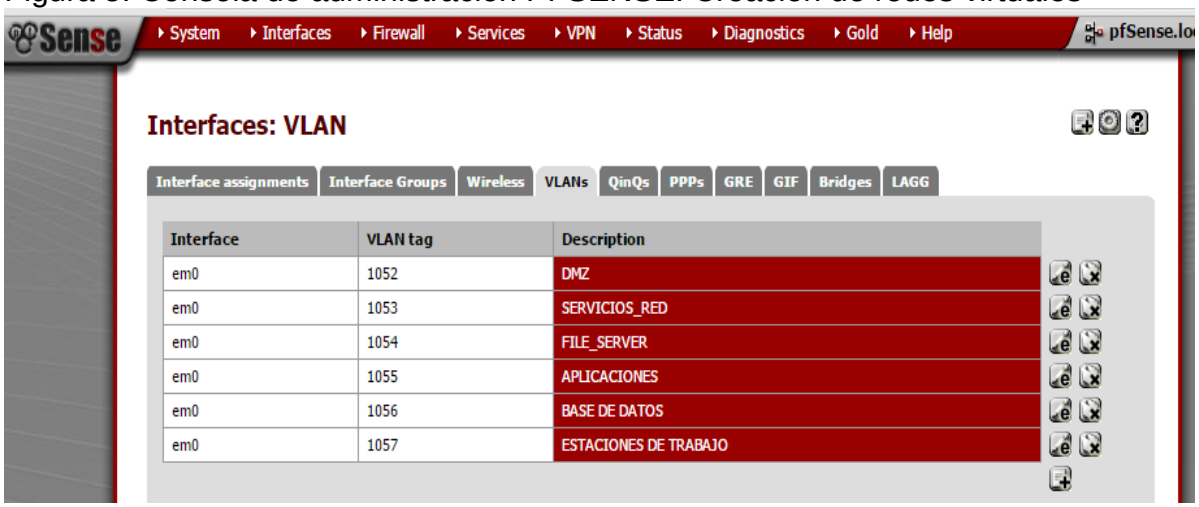
Figura 4. Consola de administración PFSENSE



Fuente: El Autor

Luego de la instalación inicial física y lógica de la solución, se procedió a realizar la creación de las redes virtuales (Vlan), según el diseño de la topología de red.

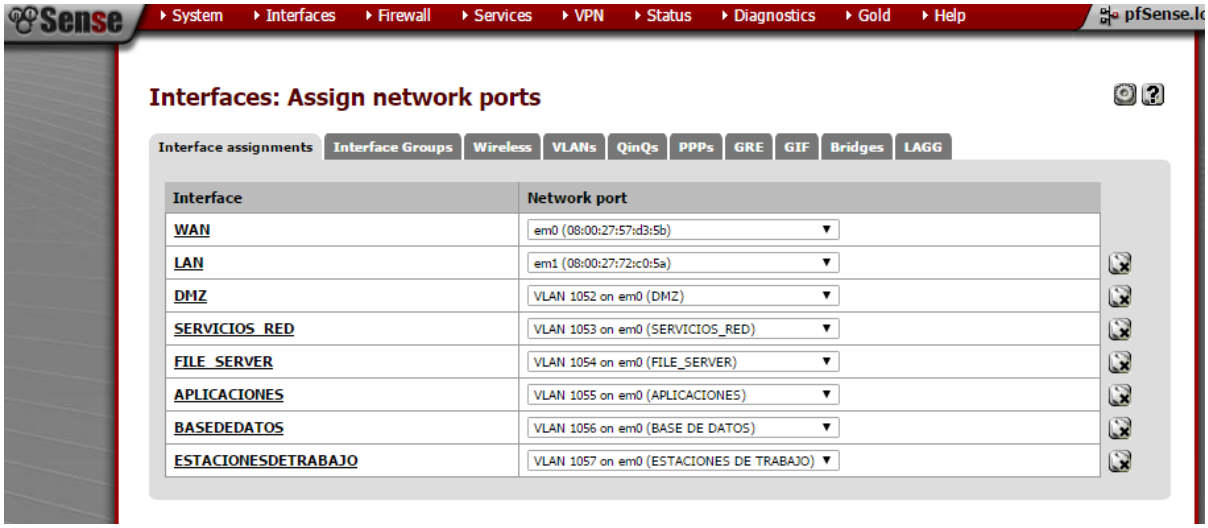
Figura 5. Consola de administración PFSENSE: Creación de redes virtuales



Fuente: El Autor

Luego de la instalación se realiza la asignación de puertos virtuales para las interfaces de red definidas en el diseño de la topologíaa segura.

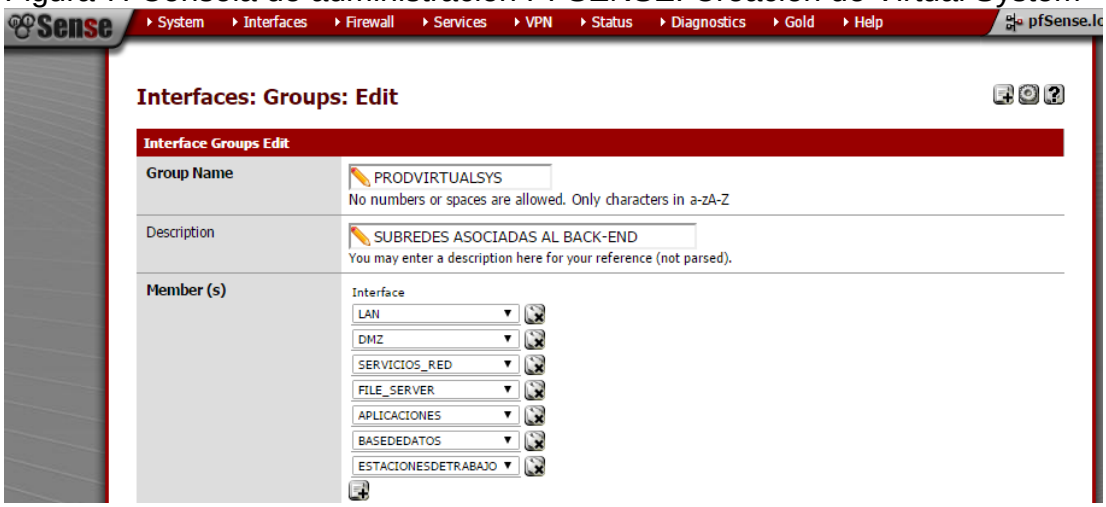
Figura 6.Consola de administración PFSENSE: Asignación de interfaces



Fuente: El Autor

Por último se configuró el virtual system que agrupa a las sub-interfaces de red que conforman el ambiente productivo de red de la zona de back-end.

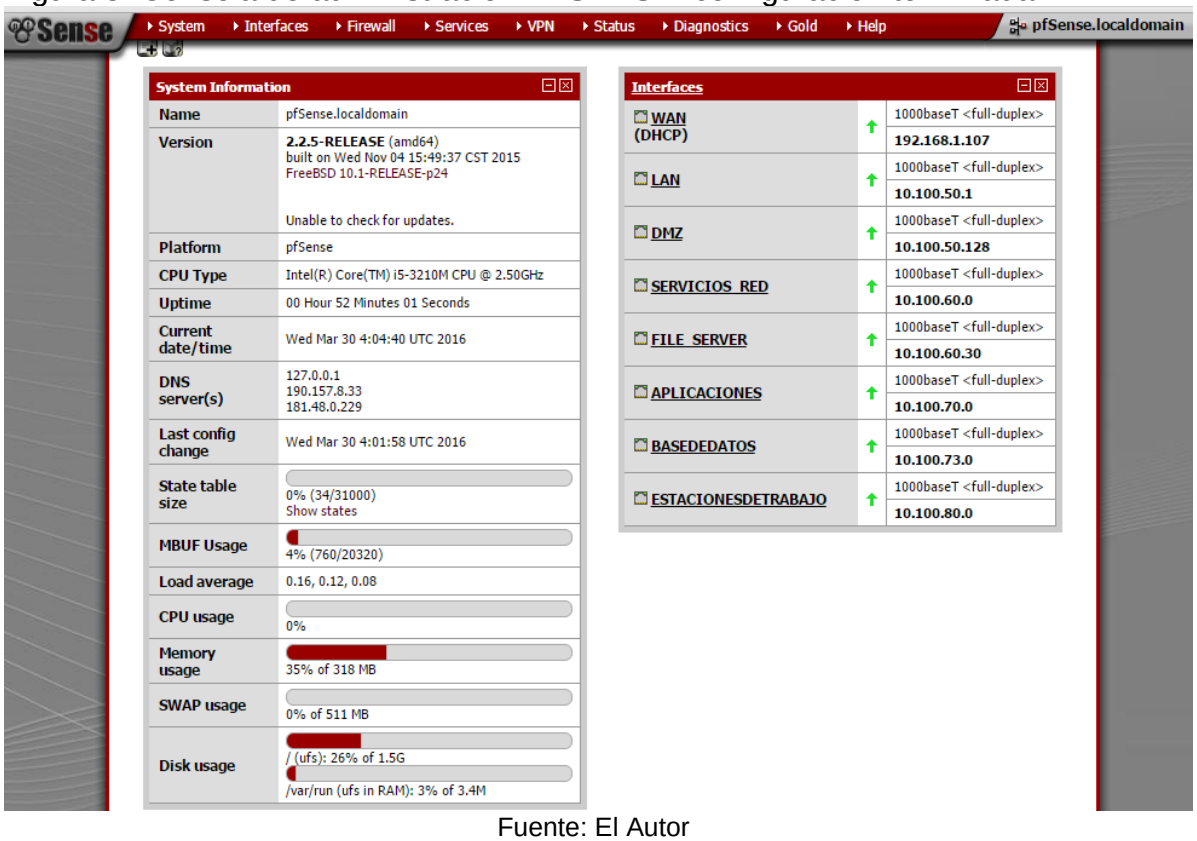
Figura 7. Consola de administración PFSENSE: Creación de Virtual System



Fuente: El Autor

La aplicación de la configuraciónn del ámbito de red finalizada en su totalidad se puede evidenciar en la consola general de administración de la solución:

Figura 8. Consola de administración PFSENSE: configuración terminada



Fuente: El Autor

5.2 INSTALACIÓN DE SOLUCIÓN DE VIRTUALIZACIÓN

La virtualización de la infraestructura de servidores se realizó bajo una configuración de alta disponibilidad con replicación, que realiza una copia incremental de la configuración de las máquinas virtuales sobre el sistema de almacenamiento de red (SAN); ésta configuración funciona de modo pasivo – activo y es capaz de restaurar la copia total de las máquinas virtuales en el servidor de contingencia y cambiar las rutas de acceso del Hypervisor en caso de fallos:

Figura 9. Consola de administración Hypervisor

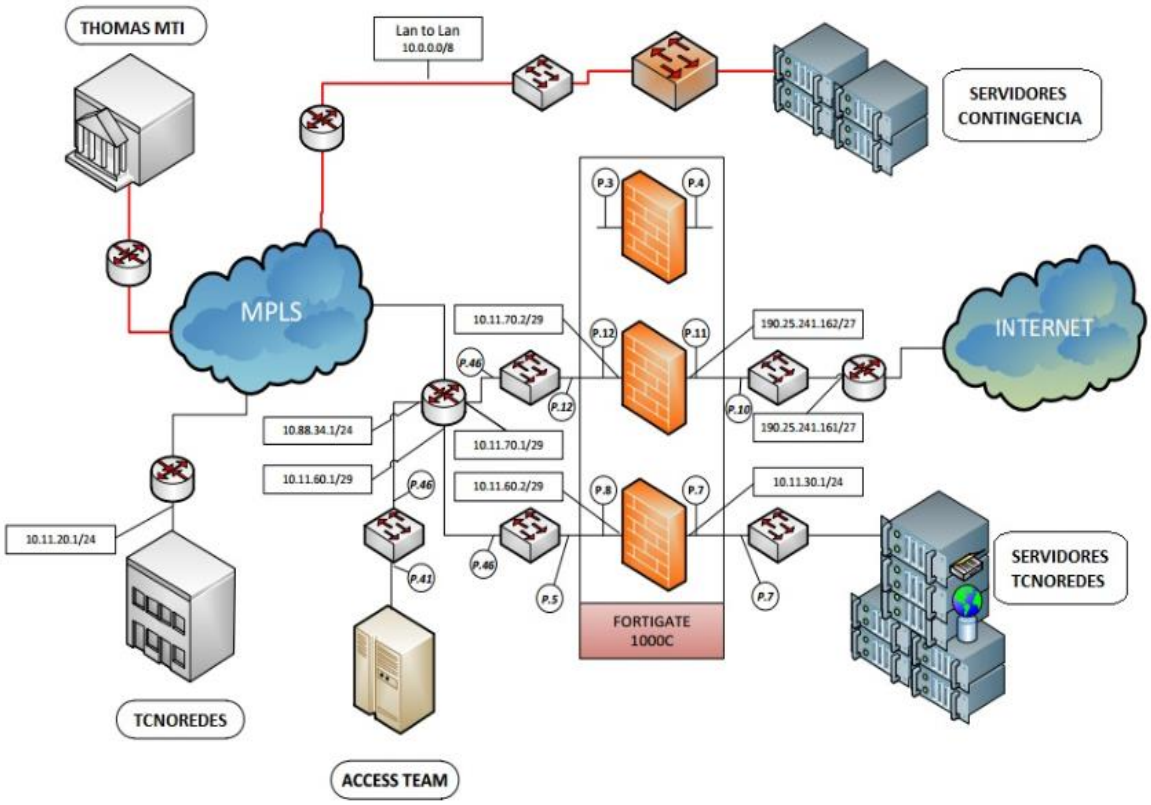
Fuente: El Autor

5.3 IMPLEMENTACIÓN DE ESQUEMA DE RENTING EN DATACENTER

Dentro del plan de optimización de los procesos de infraestructura tecnológica, se establece el alquiler de un espacio físico en dos datacenter nivel IV (Triara, Bogotá y Santa Mónica, en Cali), espacio que permitirá el alojamiento de toda la infraestructura necesaria (switch, routers, servidores, etc.) para la operación en alta disponibilidad del servicio.

5.3.1 Esquemas de conectividad y seguridad perimetral. Para enrutar la conectividad entre la sede principal de **Tecnología y Redes SAS**, los centros de datos principal y alterno y las sedes de los proveedores (Access Team, Thomas MTI) y administrar las políticas de acceso a internet, se establecen tres sistemas virtuales perimetrales, configurados dentro de la solución física de PfSense. La distribución lógica de los sistemas virtuales se describe en el siguiente diagrama.

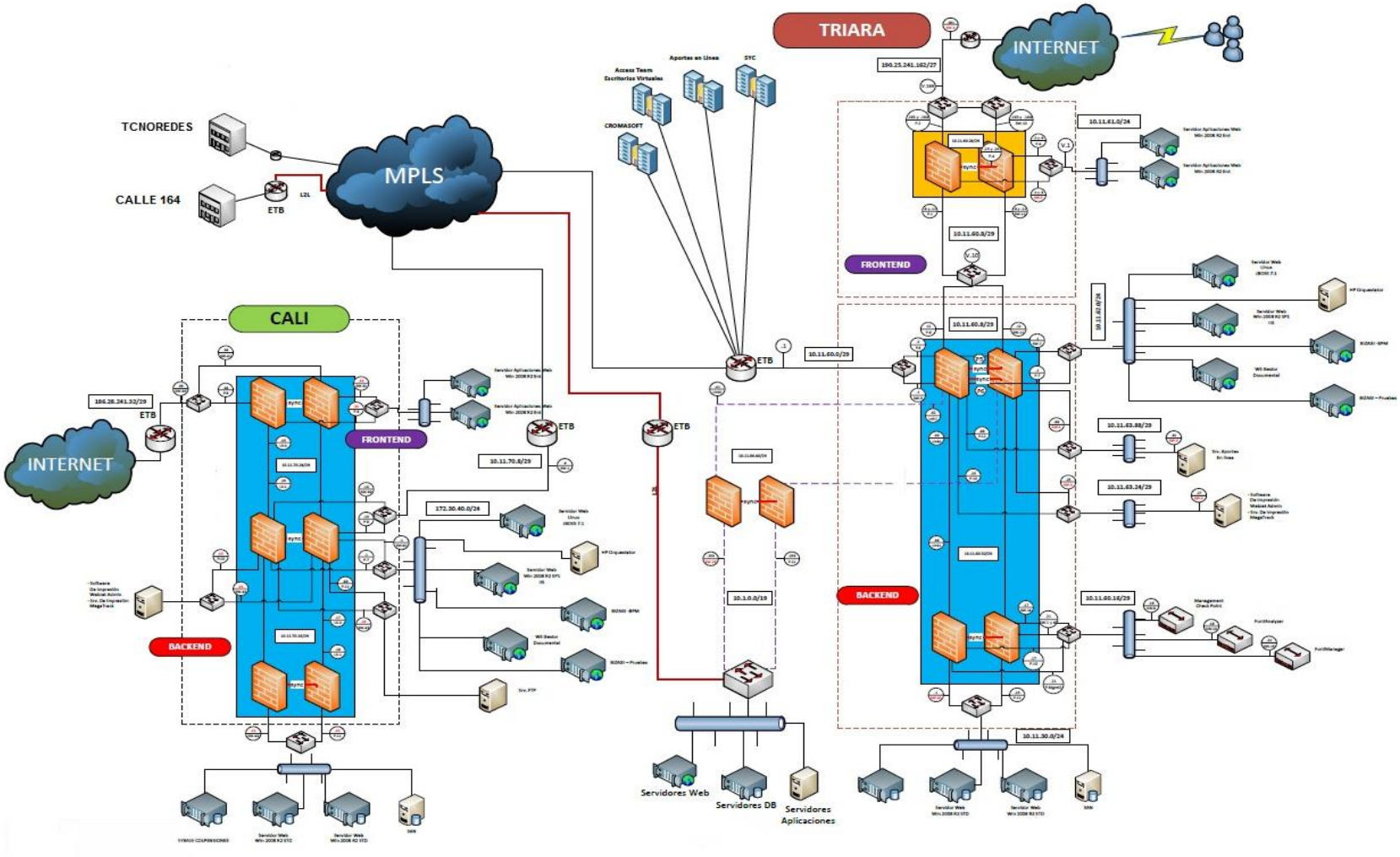
Figura 10. Firewall virtuales para Tecnoredes e internet



Fuente: El Autor

Para garantizar la seguridad e integridad de la información, se definen varias redes perimétricas en serie, alojando lo servicios que requieren de un menor nivel de seguridad en las redes más externas (DMZ), así, en caso de un posible ataque, el atacante deberá saltar por todas y cada una de ellas para acceder a la información sensible. A dicha arquitectura se le conoce como backend – frontend y se describe en el siguiente diagrama:

Figura 11. Firewall Backend y Frontend



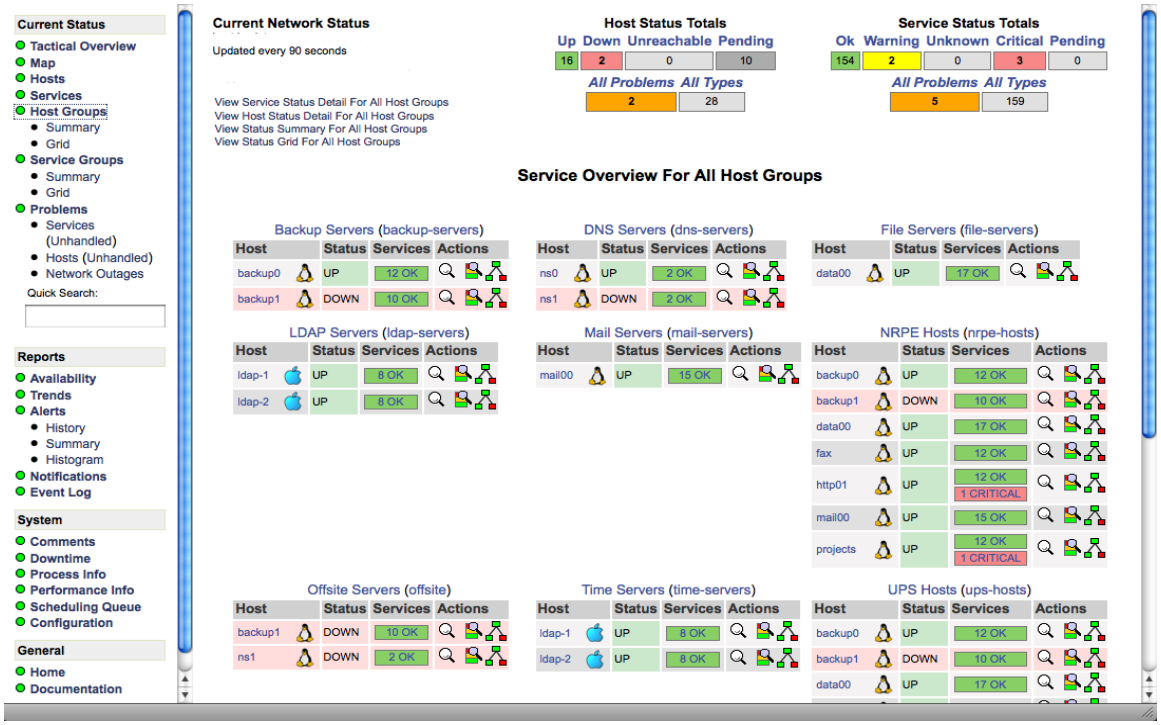
Fuente: El Autor

5.4 IMPLEMENTACION DE SOLUCIÓN MONITOREO DE INFRAESTRUCTURA BASADO EN SOFTWARE LIBRE

Luego de la implementación de las soluciones de seguridad y virtualización, se realiza la instalación de un sistema de monitoreo de infraestructura de comunicaciones y servidores, que garantice la disponibilidad de los servicios dentro de los umbrales adecuados para el óptimo desempeño de la operación. Nagios es un sistema de código abierto capaz de monitorear servicios de red esenciales (SMTP, POP3, HTTP, SNMP) y recursos de hardware como carga del procesador, estado de los discos, saturación de memoria y estado de los puertos.

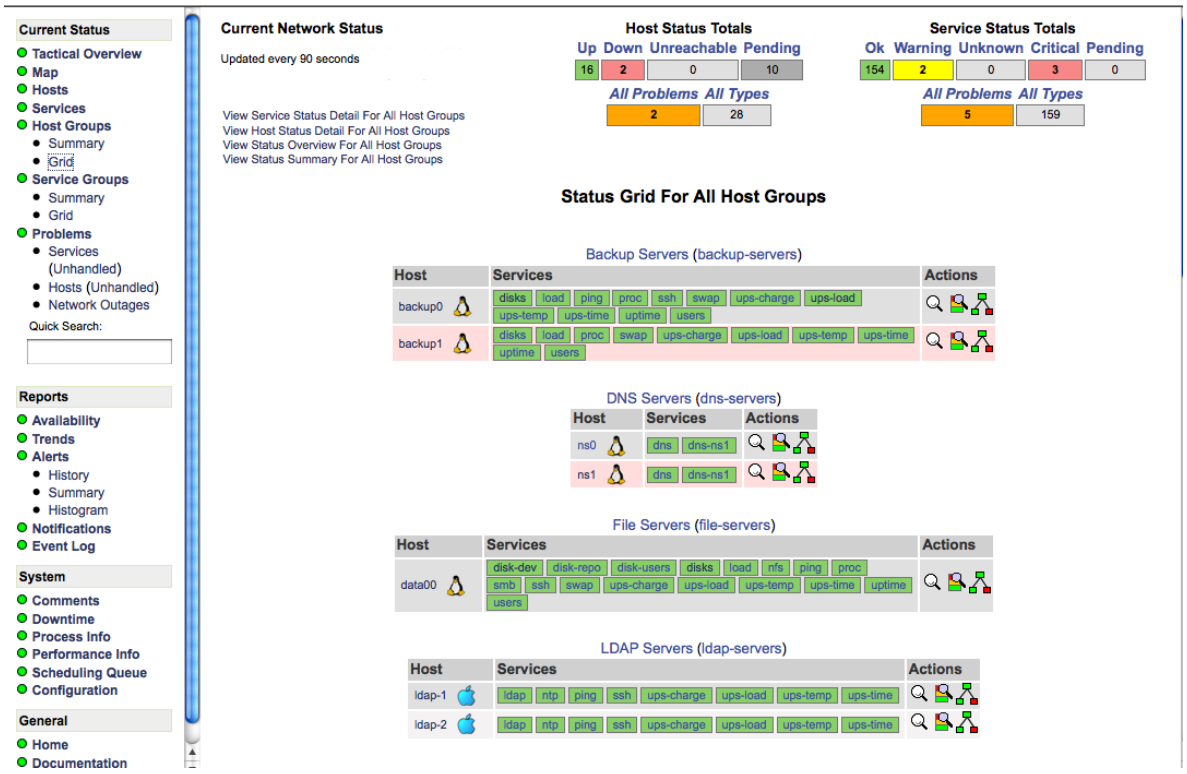
Dentro de la consola de Nagios se incluye todo el ámbito de red, que es comprendido por la infraestructura de servidores y comunicaciones implementada en esquema de datacenter, se realiza la instalación de un plug-in en cada una de las máquinas que se conecta a través de la red con la consola principal, éste pulg-in permite en tiempo real mantener actualizado el monitore de los recursos de hardware y los servicios de la infraestructura de servidores. El monitoreo de los recursos de comunicaciones se realiza a través de trazas de ICMP de manera constante, lo cual permite tener el detalle de disponibilidad de los periféricos. A continuación se detalla la consola de monitoreo de hardware y de servicios de red:

Figura 12. Consola de Nagios: Monitoreo de hardware



Fuente: El Autor

Figura 13. Consola de Nagios: Monitoreo de servicios de red.



Fuente: El Autor

6. ANÁLISIS ECONÓMICO DEL PROYECTO DE IMPLEMENTACIÓN

6.1 BENEFICIOS DEL RENTING Y DIFERENCIAS CON LA COMPRA DE INFRAESTRUCTURA Y LOS CENTROS DE DATOS PROPIOS

El servicio de renting, es una solución para las empresas que desean mantener sus equipos de TI en un espacio físico seguro y en un entorno acondicionado con energía y enfriamiento de la más alta calidad, asegurando la continuidad de su negocio; ofreciéndole un ambiente diseñado con las condiciones óptimas de operación, tales como respaldo eléctrico, seguridad física por controles de acceso, protección contra incendios y ambiente controlado (humedad y temperatura adecuadas para equipos de cómputo.

6.1.1 Ventajas del servicio

- Respaldo de la información.
- Minimiza los costos operativos.
- Seguridad y protección.
- Optimización de recursos.
- Costos mínimos de inversión.
- Aumento en la productividad.
- Disponibilidad del servicio 24/7/365.
- Tecnología de punta.
- La depreciación tecnológica es transparente para el cliente.
- Los niveles de disponibilidad de los servicios serán pactados contractualmente.

6.1.2 Adquiriendo infraestructura propia y estableciendo centro de datos local

- La compañía asume la totalidad de la depreciación tecnológica.
- Aumentan los costos de administración de la infraestructura.
- Aumentan los activos de la compañía, aumentando el valor anual de impuestos.
- Aumenta el riesgo operativo, debido a que las condiciones ambientales del centro de datos se alejan del nivel óptimo.
- Los niveles de disponibilidad de los servicios serán responsabilidad neta de la compañía.
- Dificulta la continuidad de negocio.

6.2 ANÁLISIS FINANCIERO Y PRESUPUESTO

Haciendo un análisis superficial de las posibles modalidades de implementación (renting - compra de infraestructura), es notablemente menor el riesgo del renting, toda vez que permite transferir el costo de la depreciación tecnológica al proveedor, permite la renovación tecnológica constante y asegura

contractualmente la disponibilidad de los servicios, se detalla un aproximado de costos de cada opción.

Tabla 4. Costo estimado de compra de infraestructura

CANTIDAD	ARTICULO	PRECIO UNITARIO	VALOR TOTAL
2	Servidor con Tecnologia Intel XEON 2, 8GB RAM	$ 21.000.000,00	$ 42.000.000,00
1	Unidad de almacenamiento SAN estandar	$ 27.000.000,00	$ 27.000.000,00
2	Switch 48 puertos L3 Conectividad GigaBit	$ 2.700.000,00	$ 5.400.000,00
2	UPS 4 KVA	$ 2.500.000,00	$ 5.000.000,00
2	Licencias Sistema operativo	$ 4.500.000,00	$ 9.000.000,00
1	Reacondicionamiento de centro de datos, obras civiles.	$ 25.000.000,00	$ 25.000.000,00
1	Licencia VMWARE VSPHERE	$ 14.500.000,00	$ 14.500.000,00
		TOTAL	$ 127.900.000,00

Se deben tener en cuenta también los costos mensuales de administración, operación y servicios públicos, que mensualmente redondearían $10.000.000.

Tabla 5. Costo estimado de implementación de renting.

CANTIDAD	ARTICULO	PRECIO UNITARIO	VALOR TOTAL
6	Servidores con carga de trabajo de dos procesadores X2 Núcleos y 4GB de Memoria RAM	$ 6.500.000,00	$ 39.000.000,00
1	TB de almacenamiento en Storage SAN (CDA)	$ 4.000.000,00	$ 4.000.000,00
1	TB de almacenamiento en Storage SAN (CDP)	$ 4.000.000,00	$ 4.000.000,00
1	Canal MPLS 10 Mbps con tecnologa MetroEhternet anillado redundante	$ 2.350.000,00	$ 2.350.000,00
1	Appliance de firewall PfSense 2440	$ 980.000,00	$ 980.000,00
1	HPE 5130 HI Switch Series (CDP)	$ 1.250.000,00	$ 1.250.000,00
1	HPE 5130 HI Switch Series (CDA)	$ 1.250.000,00	$ 1.250.000,00
		TOTAL	$ 52.830.000,00

En innegable el valor agregado que proporciona a la continuidad del negocio el disponer de una infraestructura en un centro de datos en condiciones ambientales, eléctricas y de seguridad física adecuadas. Adicionalmente, la opción de contar en todo momento con tecnología de punta sin tener que asumir el costo de la depreciación tecnológica.

Adicionalmente, se debe contemplar el costo operativo que implica la implementación de la solución. El consultor tendrá unos honorarios de $ 2.000.000 mensuales en un contrato por prestación de servicios, por un periodo de 4 meses, dicha discriminación se encuentra al detalle en la tabla adjunta:

Tabla 6. Salario operativo labores de consultoría e implementación.

CANTIDAD	ARTICULO	PRECIO UNITARIO	VALOR TOTAL
1	Salario Consultoria mes 1	$ 2.000.000,00	$ 2.000.000,00
1	Salario Consultoria mes 2	$ 2.000.000,00	$ 2.000.000,00
1	Salario Consultoria mes 3	$ 2.000.000,00	$ 2.000.000,00
1	Salario Consultoria mes 4	$ 2.000.000,00	$ 2.000.000,00
		TOTAL	$ 8.000.000,00

7. PLAN DE IMPLEMENTACIÓN

Luego de realizar el levantamiento de información, se diseña un plan de trabajo comprendido por las siguientes actividades:

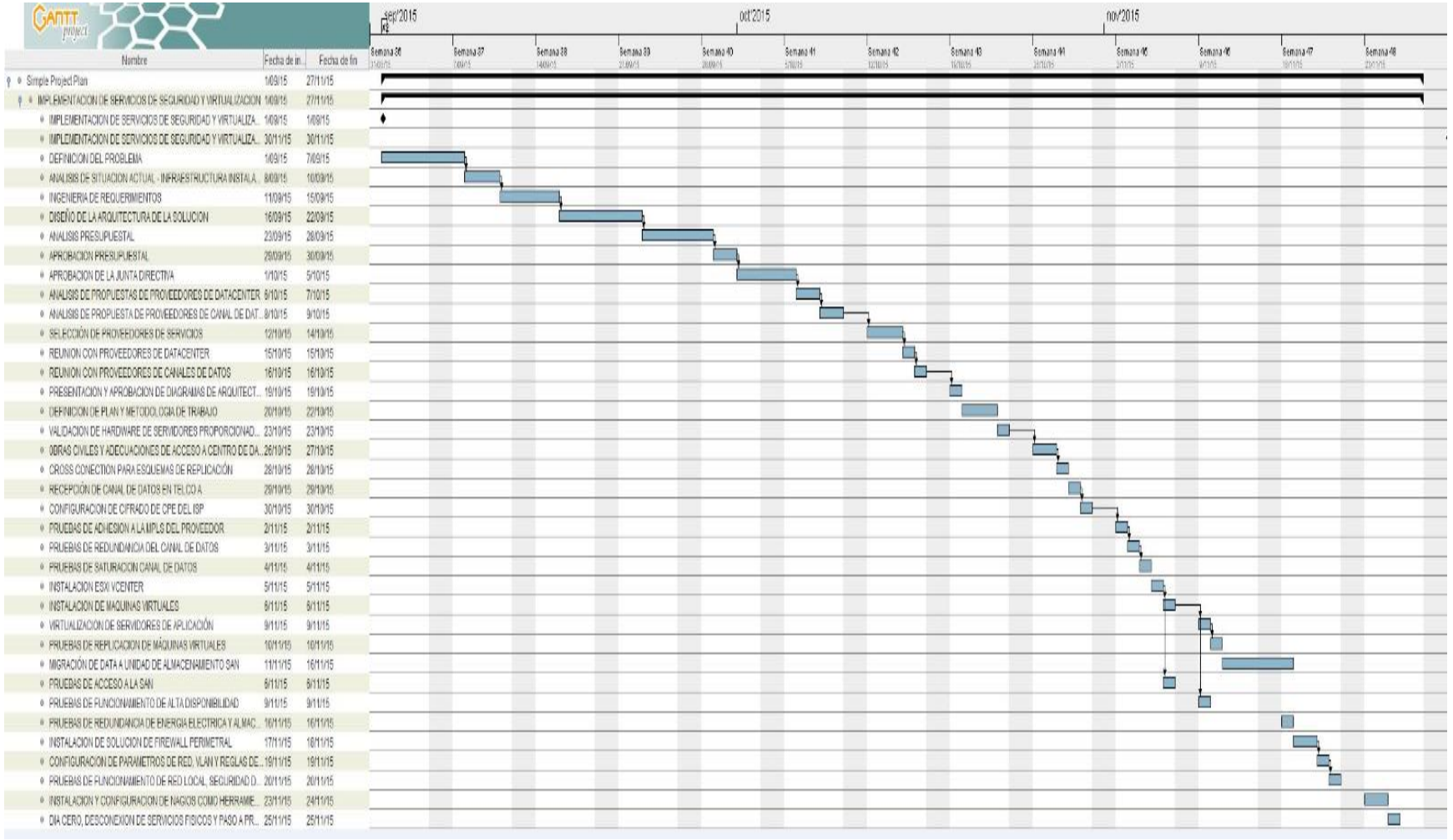
7.1 CRONOGRAMA

Para cumplir a cabalidad las metas propuestas, se define un cronograma de tiempo comprendido por 14 semanas de trabajo, ejerciendo control de actividades por semana para garantizar un seguimiento adecuado. Dicho esquema de control se plasma en la tabla siguiente.

Se realiza un esquema de cronograma apoyado en la herramienta GanttProject, en la cual se ingresan como entrada la fecha inicial del proyecto, las actividades a realizar y la duración de cada actividad, así, plasmando de manera gráfica el resumen de actividades, se puede realizar un seguimiento más efectivo de éstas.

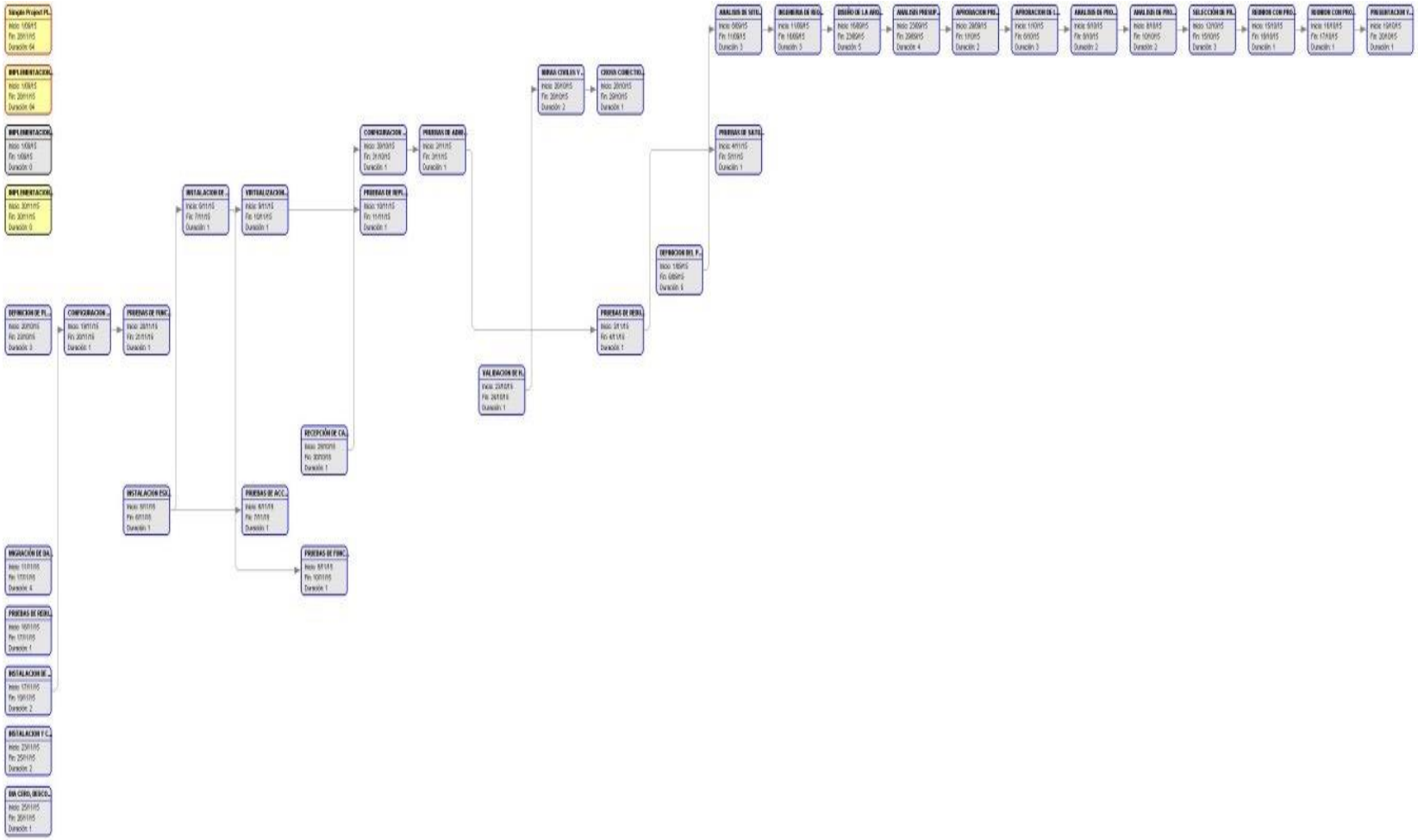
Se presentan a continuación los modelos de Gantt, para ejercer control sobre los tiempos de ejecución y de Pert, que permite realizar un seguimiento de los recursos y tiempo de ejecución del proyecto.

Tabla 7. Diagrama de Gantt de ejecución del proyecto por semanas



Nombre	Fecha de in...	Fecha de fin
Simple Project Plan	1/09/15	27/11/15
IMPLEMENTACION DE SERVICIOS DE SEGURIDAD Y VIRTUALIZACION	1/09/15	27/11/15
IMPLEMENTACION DE SERVICIOS DE SEGURIDAD Y VIRTUALIZA...	1/09/15	1/09/15
IMPLEMENTACION DE SERVICIOS DE SEGURIDAD Y VIRTUALIZA...	30/11/15	30/11/15
DEFINICION DEL PROBLEMA	1/09/15	7/09/15
ANALISIS DE SITUACION ACTUAL - INFRAESTRUCTURA INSTALA...	8/09/15	10/09/15
INGENIERIA DE REQUERIMIENTOS	11/09/15	15/09/15
DISEÑO DE LA ARQUITECTURA DE LA SOLUCION	16/09/15	22/09/15
ANALISIS PRESUPUESTAL	23/09/15	28/09/15
APROBACION PRESUPUESTAL	29/09/15	30/09/15
APROBACION DE LA JUNTA DIRECTIVA	1/10/15	5/10/15
ANALISIS DE PROPUESTAS DE PROVEEDORES DE DATACENTER	6/10/15	7/10/15
ANALISIS DE PROPUESTA DE PROVEEDORES DE CANAL DE DAT...	8/10/15	9/10/15
SELECCIÓN DE PROVEEDORES DE SERVICIOS	12/10/15	14/10/15
REUNION CON PROVEEDORES DE DATACENTER	15/10/15	15/10/15
REUNION CON PROVEEDORES DE CANALES DE DATOS	16/10/15	16/10/15
PRESENTACION Y APROBACION DE DIAGRAMAS DE ARQUITECT...	19/10/15	19/10/15
DEFINICION DE PLAN Y METODOLOGIA DE TRABAJO	20/10/15	22/10/15
VALIDACION DE HARDWARE DE SERVIDORES PROPORCIONAD...	23/10/15	23/10/15
OBRAS CIVILES Y ADECUACIONES DE ACCESO A CENTRO DE DA...	26/10/15	27/10/15
CROSS CONECTION PARA ESQUEMAS DE REPLICACIÓN	28/10/15	28/10/15
RECEPCIÓN DE CANAL DE DATOS EN TELCO A	29/10/15	29/10/15
CONFIGURACION DE CIFRADO DE CPE DEL ISP	30/10/15	30/10/15
PRUEBAS DE ADHESION A LA MPLS DEL PROVEEDOR	2/11/15	2/11/15
PRUEBAS DE REDUNDANCIA DEL CANAL DE DATOS	3/11/15	3/11/15
PRUEBAS DE SATURACION CANAL DE DATOS	4/11/15	4/11/15
INSTALACION ESXI VCENTER	5/11/15	5/11/15
INSTALACION DE MAQUINAS VIRTUALES	6/11/15	6/11/15
VIRTUALIZACION DE SERVIDORES DE APLICACIÓN	9/11/15	9/11/15
PRUEBAS DE REPLICACION DE MÁQUINAS VIRTUALES	10/11/15	10/11/15
MIGRACIÓN DE DATA A UNIDAD DE ALMACENAMIENTO SAN	11/11/15	16/11/15
PRUEBAS DE ACCESO A LA SAN	6/11/15	6/11/15
PRUEBAS DE FUNCIONAMIENTO DE ALTA DISPONIBILIDAD	9/11/15	9/11/15
PRUEBAS DE REDUNDANCIA DE ENERGIA ELECTRICA Y ALMAC...	16/11/15	16/11/15
INSTALACION DE SOLUCION DE FIREWALL PERIMETRAL	17/11/15	18/11/15
CONFIGURACION DE PARAMETROS DE RED, VLAN Y REGLAS DE...	19/11/15	19/11/15
PRUEBAS DE FUNCIONAMIENTO DE RED LOCAL, SEGURIDAD D...	20/11/15	20/11/15
INSTALACION Y CONFIGURACION DE NAGIOS COMO HERRAMIE...	23/11/15	24/11/15
DIA CERO, DESCONEXION DE SERVICIOS FISICOS Y PASO A PR...	25/11/15	25/11/15

Tabla 8. Diagrama de Pert de ejecución del proyecto por semanas



8. CONCLUSIONES

Se logró diseñar e implementar una arquitectura de red segura, basada en estándares internacionales de buenas prácticas.

Se logró realizar de manera exitosa la implementación de una política de seguridad acorde a las necesidades de la organización,

Se logra realizar un análisis técnico y financiero adecuado, identificando al detalle las necesidades y viabilidad de las posibles soluciones a dichas necesidades.

Se logran estructurar procesos de infraestructura tecnológica, serios, sólidos y de vanguardia, con tecnología de punta, brindando así respaldo y confiabilidad a los procesos misionales de la organización.

Con la implementación de la solución se garantiza la disponibilidad, confidencialidad e integridad de la información, esencia misma del negocio y el activo más valioso y preciado para éste.

Implementando infraestructura tecnológica de datacenter, se garantizan niveles de continuidad de negocio, cumpliendo así con múltiples estándares de buenas prácticas internacionales (ITIL, COBIT, TOGAF, ISO27001).

Se disminuye la depreciación tecnológica a cargo de **Tecnología y Redes SAS**, reduciendo al máximo los gastos a futuro, lo que contribuye con el objetivo financiero a largo plazo de la compañía.

Se implementa una solución de firewall perimetral de vanguardia, basada en software libre, que cumple con todos los estándares de calidad y funcionalidad necesarios para el estupendo desempeño de la operación de la organización.

Se realiza la implementación de virtualización de infraestructura sin afectar de manera alguna el normal desempeño de la operación diaria de la organización.

Se garantiza la centralización de la información de la organización, contenida en una unidad de almacenamiento adecuada, accedida con óptimos niveles de seguridad y control.

Se realiza un proceso de actualización de la infraestructura tecnológica, toda basada en principios esenciales de seguridad de la información y software libre, permitiendo así un potencial evolutivo infinito, teniendo como núcleo los estándares internacionales de buenas prácticas (ITIL, COBIT, TOGAF, ISO27001).

BIBLIOGRAFÍA

AXELOS. Global Best Practice. What is ITIL Best Practice? [en línea] Disponible en Internet en: https://www.axelos.com/best-practice-solutions/itil/what-is-itil

BORBON SANABRIA, Jeffrey Steve. Buenas prácticas, estándares y normas [en línea] Revista Seguridad 1 251 478 [Citado Julio 25, 2011] Nº 11. Disponible en internet: http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

CAPACITACIÓN ITL. Itil versión 3 [en línea] ITIL V3 [Citado Junio 7, 2016] Disponible en internet: capacitacionitil.blogspot.com/p/itil-v3-en-itil-v3-reestructura-el.html

COTECNA Trade Services. Certificación ISO 27001 [en línea] Disponible en internet_
http://www.cotecna.com.ec/~/media/Countries/Ecuador/Documents/Brochure-iso-27001-cotecna-ecuador-FINAL.ashx?la=es-ES

FERRER, Jorge y FERNÁNDEZ SANGUINO, Javier. Seguridad, informática y software libre [en línea] Hispalinux. Disponible en internet:
http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf
https://www.pfsense.org/getting-started/

ISACA.ORG. What is Cover 5 [en línea] [Publicado Junio 30, 2016] Disponible en Internet: https://cobitonline.isaca.org/about

ISO/IEC 27001 - Information security management [en línea] [Publicado Noviembre 27, 2013] Disponible en internet: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

PFSENSE.ORG. Take a tour. Gettin started [en línea] Disponible en Internet en:
PLCT S.A. de C.V. Virtualización [en línea] Disponible en internet: http://plct.com.mx/index.php/servicios/virtualizacion

SGSI. ISO/IEC 27005 Gestión de Riesgos de la Seguridad la información [en línea] Blog especializado en sistemas de gestión de seguridad de la información [Citado Enero 31, 2014] http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/
VM WARE INC. Tipos de Virtualización [en línea] Disponible en internet: http://www.vmware.com/co/virtualization/getting-started.html

VM WARE INC. Virtualización [en línea] Disponible en internet: [Publicado Junio 30, 2016] http://www.vmware.com/co/virtualization/overview

WIKIPEDIA. Definición ISO/IEC 27001 [en línea] [Citado Septiembre 14, 2011] Disponible en internet: https://es.wikipedia.org/wiki/ISO/IEC_27001

WIKIPEDIA. Definición ISO/IEC 27002 [en línea] [Editado Mayo 8, 2016] Disponible en internet: https://es.wikipedia.org/wiki/ISO/IEC_27002

WIKIPEDIA. Information Tecnology Infraestructure Library [en línea] [Editado Junio 7, 2016] Disponible en internet: https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Historia_y_precursores_de_ITIL

WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas [en línea] [Editado Abril 19, 2016] Disponible en internet: https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas