ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

Diseño y propuesta técnica-económica de la red con voz sobre IP y datos apoyados en la norma ISO/IEC 27001:2013 para la empresa de comercio exterior "KUEHNE-NAGEL división PERECIBLES"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMATICOS Y DE COMPUTACIÓN

LUIS ANDRÉS VILLAVICENCIO PÉREZ
luisvp59@hotmail.com

DIRECTOR: ING. CESAR GUSTAVO SAMANIEGO BURBANO, MSc.
gustavo.samaniego@epn.edu.ec

QUITO, Julio 2015

DECLARACIÓN

Yo, Luis Andrés Villavicencio Pérez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la Normativa institucional vigente.

_____

Luis Andrés Villavicencio Pérez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Andrés Villavicencio Pérez, bajo mi supervisión.

_____

Ing. Msc. Gustavo Samaniego
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A mi director de tesis, Ing. Cesar Samaniego por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia, fundamentales a la hora de realizar este proyecto.

Agradecimiento infinito a mi familia quienes siempre me apoyan para el cumplimiento de mis metas

Al personal de la empresa SATELITE.COM e ISEC Ecuador por brindarme las facilidades para la culminación con éxito de este proyecto.

Luis

DEDICATORIA

Este trabajo se lo dedico a Dios quien me ha dado la fortaleza para levantarme en momentos en que la única salida era tirar la toalla.

A mis padres que me han formado como un hombre íntegro, quienes me han comprendido y guiado en momentos muy difíciles.

A mis hermanos que estuvieron velando por mi bienestar.

A todos mis amigos con quienes he compartido momentos muy buenos y que me animaron para seguir adelante.

A mis dos sobrinos, Palita y Nico quienes aún no se dan cuenta de este logro pero su presencia me anima cada día.

Luis

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación tiene como objetivo realizar un análisis y diseño de la red corporativa de la empresa de comercio exterior "KUEHNE+NAGEL división PERECIBLES".

En el primer capítulo, se presenta una descripción y caracterización de la empresa para conocer antecedentes, situación actual con respecto a la infraestructura tecnológica, cableado estructurado, telefonía tradicional utilizada; al mismo tiempo realizar un análisis de crecimiento tecnológico como en el crecimiento en el número de usuarios. Con base en estos aspectos se realiza el respectivo análisis de requerimientos para posteriormente definir el diseño de la red y el dimensionamiento de dispositivos y soluciones tecnológicas necesarios.

En el capítulo dos, se diseña la red corporativa incluyendo la red de datos, la red inalámbrica, el acceso remoto y la red de telefonía sobre IP con base en los requerimientos acordados con la empresa y proporcionando características de disponibilidad, redundancia y movilidad para los usuarios, además de seguridad a toda la red siguiendo los lineamientos que proporciona la metodología SAFE CISCO.

En el tercer capítulo, se realiza un análisis de costos de las soluciones proporcionadas, haciendo una completa ingeniería de detalle. Se incluyen los costos de instalación y mantenimiento de la nueva red de voz, la instalación y certificación del cableado estructurado para la red actual y las soluciones para asegurar el cumplimiento de seguridad de la información.

En el capítulo cuatro se establecen las conclusiones que se derivan después de la realización del proyecto, incluyéndose, además, las recomendaciones que se plantean tanto para la empresa como para la ejecución de proyectos similares.

Al final, como elementos complementarios, se encuentran los anexos, que corresponden a diagramas, Tablas y documentos utilizados a lo largo de este proyecto.

1. CAPITULO 1

EVALUACIÓN DE LA SITUACIÓN ACTUAL DE LA EMPRESA

1.1. ANTECEDENTES

Kuehne+Nagel S.A. ha estado establecida en el Ecuador por más de 15 años y por más de 100 años a nivel mundial. El giro del negocio de S.A. ha sido, a lo largo de ese tiempo, proveer servicios de flete internacional aéreo y marítimo, aduanas, logística y transporte local. En el Ecuador, posee oficinas en las dos ciudades más importantes del Ecuador como son Quito y Guayaquil.

Ante las necesidades de un mercado en constante cambio la empresa se vio en la necesidad de expandir su área de actividad hacia la exportación de flores y otros productos perecibles, formando así alianzas estratégicas con varias empresas que se dedican a esta actividad.

En el año 2012, se creó legalmente la división PERECIBLES de la empresa KUEHNE+NAGEL, las empresas que constituían dicha división en un principio fueron MASTER TRANSPORT S.A, TAO S.A y TAISA S.A.

Master Transport S.A. se integró a esta alianza estratégica brindando personal e instalaciones que prestaban el servicio de exportación de perecibles; en el caso de Tao S.A y Taisa S.A esencialmente fueron integradas por motivos logísticos, es decir, debido a que contaban con instalaciones apropiadas para el negocio.

Los trabajadores de las tres empresas mencionadas pasaron a formar parte de KUEHNE+NAGEL S.A, lo que desde el punto de vista tecnológico implicó ciertos cambios que serán analizados más adelante en este proyecto.

1.1.1 MISIÓN DE LA EMPRESA

"The global logistics network is our strongest asset. Dedication, integration and innovation are at the heart of our business philosophy. Focused on our customers' needs we provide integrated logistics solutions of outstanding quality and operational excellence – we are the extension of your business."[1]

KUEHNE+NAGEL, es una de las compañías líder de logística en el mundo, ofrece soluciones integrales a través de la cadena de abastecimiento y ha pasado de ser un agente de carga internacional a ser un proveedor global líder en soluciones integrales de la cadena de abastecimiento para una gama de industrias.

1.1.2 VISIÓN DE LA EMPRESA

"Ser el mejor proveedor de soluciones logísticas para nuestro clientes dentro de la red global de KUEHNE+NAGEL, lográndolo por medio de personas altamente calificadas y motivadas"

1.1.3 OBJETIVOS DE LA EMPRESA

Kuehne+Nagel se esfuerza por asegurar un entorno de la cadena de suministro estable y previsible en el que la empresa y sus clientes pueden seguir sus actividades sin interrupción o daño y sin temor a la perturbación de la carga confiada a lo largo de la cadena de suministro.

Adicionalmente se determinó objetivos específicos que son:

- Satisfacer las necesidades de nuestros clientes eficaz y eficientemente.
- Asociarse a los mejores proveedores del mundo para darle a nuestros servicios un valor agregado que se traduzca en beneficios para nuestros clientes y personal de la empresa.

---

[1] http://www.kn-portal.com/about_us/about_us/mission_statement/

- Aumentar nuestra cartera de clientes nacional e internacional.
- Brindar a nuestros empleados la oportunidad de crecer junto a la empresa.
- Generar una acción responsable hacia los recursos naturales y la sociedad misma.

1.1.4 VALORES INSTITUCIONALES

- Actuar como una extensión del negocio de nuestro cliente
- Mejorar constantemente
- Colaborar
- Mantener nuestras promesas
- Responsabilizarse de las actividades
- Controlar los costos
- Respetar a los demás
- Divertirse

1.1.5 LOCALIZACIÓN DE LA EMPRESA

A partir del proceso legal que se explicó en el punto 1.1, se inicia la formación de KUEHNE+NAGEL división PERECIBLES. En un principio las empresas mencionadas estuvieron localizadas en el sector del antiguo Aeropuerto “Mariscal Sucre”, específicamente MASTER TRANSPORT y TAO estaban ubicadas en la calle Gonzalo Gallo y Av. La Prensa y las oficinas de TAISA se encontraban localizadas en la Av. Río Amazonas y calle Palora. En febrero de 2014, todas las oficinas y operación nacional e internacional de pasajeros y carga del aeropuerto se trasladó a la parroquia de Tababela, ubicada a unos 18 kilómetros al este de la ciudad de Quito, donde se estableció el nuevo Aeropuerto Internacional “Mariscal Sucre”. Este sector comercial y de logística es conocido como “Tabacarcen” quedando solo KUEHNE+NAGEL como compañía principal, la misma que está localizada en la ciudad de Quito, en la Av. Irlanda N.500 y República del Salvador. A partir de este movimiento tanto TAO como TAISA fueron fusionadas dentro de MASTER TRANSPORT S.A. convirtiéndose en la empresa KUEHNE+NAGEL división PERECIBLES.

1.2 DESCRIPCIÓN DE LA SITUACIÓN DE LA EMPRESA

En esta sección se detallará los productos o servicios que brinda la empresa, así como la situación del personal, la infraestructura tecnológica, el direccionamiento IP de la empresa KUEHNE+NAGEL división PERECIBLES, de manera que se pueda tener una idea más clara de la situación actual de la empresa y así poder establecer la propuesta de diseño de la red corporativa segura, que constituye el objetivo de este proyecto.

1.2.1 DESCRIPCIÓN DE LOS PRODUCTOS O SERVICIOS

Entre los principales servicios que la empresa brinda se encuentran los siguientes:

- Gestionar el servicio de logística integral para cada proceso en el que se encuentra el producto perecible.
- Reportar al cliente el estado completo y detallado del envío.

Según se pudo conocer después de las visitas realizadas a KUEHNE+NAGEL, estas actividades no serán diferentes de las que se realicen cuando la división PERECIBLES esté totalmente operativa en Tababela.

1.2.2 PERSONAL DE LA EMPRESA

Es necesario entender primero el funcionamiento interno y las áreas en las cuales se encuentra dividida la empresa, ya que esto influirá directamente en la forma como se diseñarán y organizará la red corporativa.

El proceso de fusión de las empresas mencionadas bajo una sola organización denominada KUEHNE+NAGEL división PERECIBLES es el objetivo de la alta gerencia de KUEHNE+NAGEL S.A. ya que al contar con instalaciones más amplias las dos empresas se constituyen en complementarias entre sí.

Organizacionalmente, KUEHNE+NAGEL división PERECIBLES está divida en 3 departamentos que son: 1. Operaciones, 2. Coordinación, y 3. Atención al Público, cada uno de ellos con su respectivo gerente o director de área; sin embargo, tanto física como tecnológicamente no existe división entre estos tres departamento por lo que se considera que existe una sola área funcional. Dicho esto, el detalle de la distribución de los trabajadores, es decir los usuarios que hacen uso de la red, se describe en la Tabla 1.

Oficina	Horario	Cantidad máxima de personas por turno
KUEHNE+NAGEL división PERECIBLES	Matutino	50
KUEHNE+NAGEL división PERECIBLES	Nocturno	15

Tabla 1. Cantidad de usuarios de la red en MASTER TRANSPORT[2].
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

El número de usuarios descrito en las Tabla 1 no es un número fijo ya que en ocasiones el personal de la mañana realiza cambios en los horarios para laborar en el turno nocturno y viceversa, pero dichas variaciones no afectan sustancialmente el desarrollo del proyecto.

Por otro lado, es importante destacar que no existe un departamento de sistemas constituido como tal, sino que las actividades que normalmente corresponden a este departamento, son ejecutadas por una sola persona, el Ing. Cristian Altamirano, quién de aquí en adelante se mencionará como “Departamento de Sistemas de KUEHNE+NAGEL división PERECIBLES o Departamento de sistemas de KN” como fuente de información.

[2]Información proporcionada por KUEHNE NAGEL EC.

1.2.3 INFRAESTRUCTURA TECNOLÓGICA

1.2.3.1 Hardware

Dentro de la empresa KUEHNE+NAGEL división PERECIBLES, para el desempeño de las laborares diarias de los trabajadores se necesitan equipos que son parte de la red interna y para las conexiones entre oficinas. En la Tabla 2 se muestra el inventario de equipos de usuario final dentro de la empresa.

Oficina	Descripción	Especificaciones técnicas	Cantidad
KUEHNE+NAGEL división PERECIBLES	Computador de escritorio.	- Intel Core i5 - Memoria: 4GB - Disco Duro: 320 GB	50

Tabla 2. Inventario MASTER TRANSPORT[3]
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

1.2.3.2 Central telefónica.

Anteriormente, en el antiguo Aeropuerto Mariscal Sucre, KUEHNE+NAGEL división PERECIBLES brindaba el servicio telefónico tradicional, en la Tabla 3 se describe dicha central.

[3]Información proporcionada por KUEHNE NAGEL EC

Oficina	Descripción	Especificaciones técnicas
KUEHNE+NAGEL división PERECIBLES	Central telefónica PANASONIC KX-TA308	- Capacidad base 3 líneas analógicas externas y 8 Extensiones Híbridas. - Posibilidad de incrementar la capacidad de su sistema hasta 6 líneas externas y 24 extensiones

Tabla 3. Central Telefónica.
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

1.2.3.3 Servidores

En las nuevas instalaciones, el área asignada por la empresa KUEHNE+NAGEL división PERECIBLES para la ubicación del DataCenter[4] no es la óptima ya que se encuentra en las mismas dependencias en las que laboran los trabajadores, además de otras deficiencias que se detallarán más adelante, en la Tabla 4 se indica el servidor disponible en estas instalaciones.

Oficina	Áreas de trabajo	Descripción	Cantidad
KUEHNE+NAGEL división PERECIBLES	Logística	Servidor DELL POWER EDGE 2900 DC XEON	1

Tabla 4. Servidor VMWare ESXi
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

1.2.3.3.1 Características técnicas del servidor.

- Tipo: Servidor de Torre 5U
- Procesador: Intel Xeon 5300 con 2.86 GHz
- Memoria: 24 GB

[4]DataCenter: es el centro tecnológico de toda empresa, construido como un ambiente apropiado y seguro, en el cual se albergan los servidores

- Disco: 2 TB
- Interfaz red: NIC Gigabit Ethernet Broadcom (3)

Este servidor sirve como alojamiento para 2 máquinas virtuales, como se detalla en la Figura 1, creadas bajo la plataforma de virtualización VMWARE, se trata del hipervisor vSphere ESXi 5.1

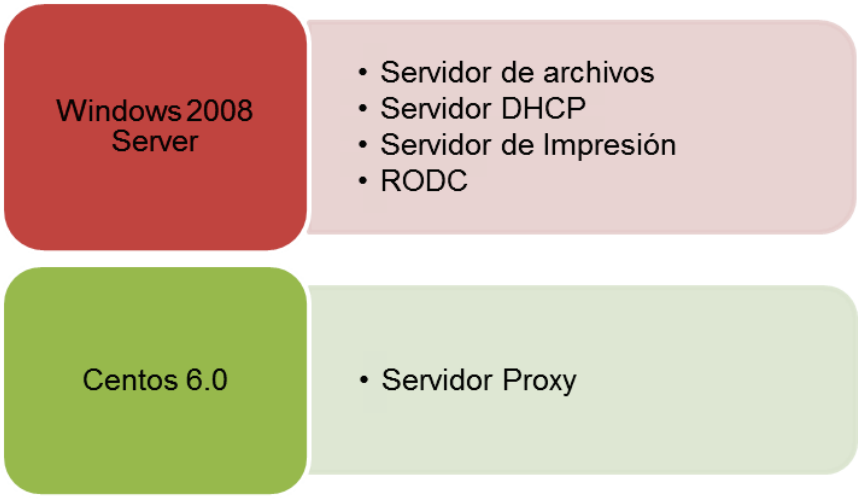


Figura 1. Servidores Virtualizados
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

Al tratar con una empresa multinacional, se ha visto en la necesidad de instalar un RODC[5] con el fin de brindar inicios de sesión a los diferentes equipos pero sin tener un controlador de dominio localmente instalado.

1.2.3.3.2 Características técnicas de Máquinas virtuales.

Windows Server 2008 R2:

- Número Procesadores: 4
- Memoria: 4 GB

[5]Read-Only Domain Controller

- Espacio en Disco: 500 Gb

Centos 6.0:

- Número Procesadores: 4
- Memoria: 4 GB
- Espacio en Disco: 80 Gb

1.2.3.4 Equipos de conectividad

En la Tabla 5 se pueden observar los equipos de conectividad disponibles en KUEHNE+NAGEL división PERECIBLES. Posteriormente se realizará el análisis sobre si estos equipos pueden ser utilizados para el diseño de la red corporativa a proponer.

Localidad	Equipo	Marca	Modelo
KUEHNE+NAGEL división PERECIBLES	Router	Cisco	891
	Switch	3com	4500

Tabla 5. Equipos de comunicación
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

1.2.3.5 Software

La empresa tiene paquetes de software licenciado como sistema operativo “Windows 7 Professional” de 32 y 64 bits, además de software de utilitarios como Microsoft Office 2010. La empresa cuenta con 60 licencias tanto para el Sistema Operativo como el paquete Microsoft Office, además se disponen de 1 licencia Windows Server 2008 Standard Edition. En la Tabla 6 se detallan los paquetes de software licenciado existente.

Oficina	Áreas de trabajo	Descripción	Cantidad
KUEHNE+NAGEL división PERECIBLES	Logística	• Windows Professional 7 • Microsoft Office 2010	60

Tabla 6. Licencias de software licenciado[6]
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

Existen varias aplicaciones instaladas en los equipos, en casi todos los casos se trata de software freeware como:

- Antivirus (avast, avira entre otros)
- Reproductores de música (winamp).
- Lectores de archivos PDF (Adobe AcrobatReader).
- Programas P2P (ares).
- Otros (skype, atubecatcher, etc).

El objetivo de detallar este tipo de software es puntualizar que no existen políticas de la empresa que permitan, prohíban o restrinjan el uso de software que pueda ser perjudicial para el rendimiento de la estación de trabajo y para la red en general.

1.2.4 DIRECCIONAMIENTO IP

El direccionamiento IP en una red es prioritario para que haya conectividad entre cada uno de los nodos de la red. La empresa KUEHNE+NAGEL división PERECIBLES tiene asignado un rango determinado de direcciones del segmento de red, como se observa en la Tabla 7. En esta Tabla se incluyen direcciones IP de servidores, usuarios e impresoras.

[6]Información proporcionada por KUEHNE NAGEL

Oficina	Áreas de trabajo	Segmento de red	Puerta de enlace	Mascara de red
KUEHNE+NAGEL división PERECIBLES	Logística	10.5.130.0	10.5.130.249	255.255.255.0

Tabla 7. Direccionamiento IP[7]
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

La asignación de direcciones IP para los dispositivos de red es realizada de manera dinámica.

1.2.5 RED INALÁMBRICA

Dado el auge de los dispositivos inalámbricos como teléfonos inteligentes o "smartphones" y tabletas, y con el fin de prestar un servicio para los visitantes, la empresa posee una red inalámbrica que se encuentra disponible tanto para los usuarios locales como para los visitantes.

Es necesario señalar que la red Wireless también será tomada en cuenta en temas de seguridad de la información con el fin de que esta red no se convierta en un riesgo de seguridad para la empresa y la información que maneja.

1.3 ANÁLISIS DE CRECIMIENTO

En sus inicios las empresas, antes de conformar empresa KUEHNE+NAGEL división PERECIBLES, el número de personas laborando en las tres empresas alcanzaba los 40 usuarios, a partir del proceso mencionada en el punto 1.1 se llegó a los 50 usuarios.

[7]Información proporcionada por KUEHNE NAGEL EC

Con base en las entrevistas realizadas, se determinó que el crecimiento proyectado será de entre el 10 y el 15 %, por lo tanto el crecimiento alcanzará los 60 usuarios como se muestra en la Figura 2.

El diseño de la red considerará equipos de conectividad, topologías, ancho de banda y cableado estructurado los mismos que, de manera conjunta, permitan proveer un excelente servicio a los usuarios de la red. De esta manera se garantiza que, en caso de un eventual incremento del personal por fuera de lo establecido al momento o de la ampliación de la KUEHNE+NAGEL división Perecibles, la operatividad de la red y de todos sus servicios no se vea afectada ni en su funcionamiento ni en su rendimiento.

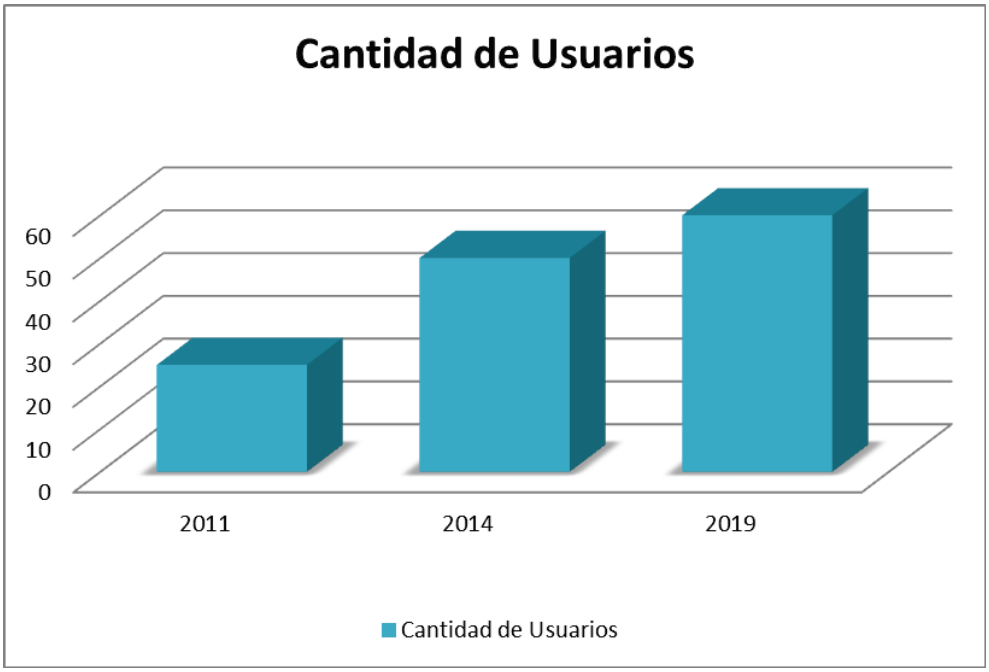


Figura 2. Analisis de crecimiento.
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

1.4 ANÁLISIS DE REQUERIMIENTOS

Con el fin de proveer a la empresa de un diseño adecuado de la infraestructura de red de KUEHNE+NAGEL división PERECIBLES, es importante realizar un correcto análisis de requerimientos, ya que de esa manera el diseño de la red

será más preciso para las necesidades de la empresa con un adecuado dimensionamiento de soluciones de hardware o software, según amerite.

Considerando esto, las soluciones a los requerimientos estarán encasillados principalmente en asegurar los tres pilares de la norma ISO/IEC 27001:2013 los cuales son integridad, disponibilidad y confidencialidad, sin descuidar el rendimiento de todos los servicios que la red corporativa debe proporcionar, en este caso puntual, el servicio de VoIP.

Con base en el análisis y descripción de la empresa realizada anteriormente, además de las visitas a la empresa para recopilación de información, los requerimientos establecidos son los siguientes:

1.4.1 REQUERIMIENTOS FÍSICOS

Previo a definir los requerimientos, es necesario establecer cuáles son las deficiencias encontradas en las visitas realizadas a la empresa:

- El cableado estructurado vertical ha sido implementado por la empresa QUIPORT, se ha dispuesto que las propias empresas diseñen el cableado estructurado horizontal con base en estándares. Este cableado estructurado horizontal hace referencia al cableado desde el Datacenter, servidores y equipos de comunicación hacia las estaciones de trabajo o puntos finales.

- El espacio en el cual se encuentra el DataCenter, aunque es un espacio aislado, no dispone de todas las seguridades físicas en cuanto al acceso al mismo

- El rack en el cual se encuentran los equipos físicos de comunicaciones no posee cableado estructurado certificado.

- Los equipos de comunicación tiene varios años de funcionamiento, en algunos casos más años de los recomendados por el fabricante.

- No existe un UPS que suministre energía eléctrica, cuando se corte el flujo de energía hacia los servidores y puntos finales, con el fin de salvaguardar la información que esté en uso, además de, proteger al hardware ante estos estos peligros.

- El cableado estructurado es relativamente antiguo como para brindar el servicio de Voz sobre IP con total eficiencia.

Las observaciones anteriormente descritas, llevan a hacer un breve resumen de los requerimientos físicos, estos son:

- Diseñar y proponer cableado estructurado horizontal certificado.
- Plantear un sistema de control y seguridad de acceso físico al DataCenter.
- Proporcionar un sistema de protección en caso de falla en la energía eléctrica.
- Adecuar el DataCenter cumpliendo las mejores prácticas recomendadas (cableado estructurado de calidad y certificado, etiquetado adecuado).

1.4.2 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

Los requerimientos de seguridad de la información para la empresa han sido determinados con base en lo establecido en la norma ISO/IEC 27001:2013.

Según la norma ISO/IEC 27001:2013, un proceso de análisis y evaluación de riesgos efectivo buscará atender las necesidades reales de la organización e involucrará a los dueños de la información (por lo regular, los dueños de los procesos de negocio), con el fin de identificar los controles que cumplan sus necesidades.

En el presente proyecto no se realizará un análisis de riesgos con todas las etapas tal y como recomienda la norma ISO/IEC 27005, sin embargo, para determinar los requerimientos de seguridad de la información, se apoyará en el

triángulo CID establecido por ISO/IEC 27001, que contiene los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad los mismas que interactúan entre sí durante cada uno de los procesos de negocio de la empresa, como se observa en la Figura 3.

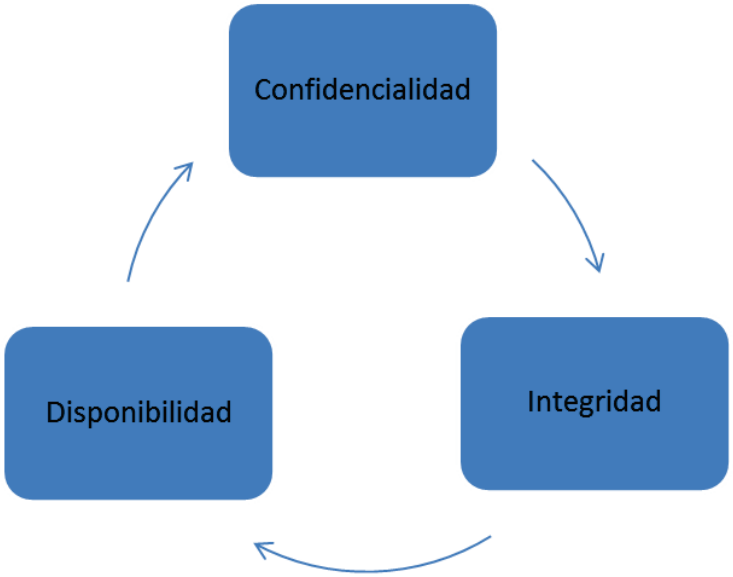


Figura 3. Objetivos de aseguramiento de seguridad de la información
Fuente: NORMA ISO/IEC 27001
Elaborado por el autor

Para entender de mejor manera cada uno de los conceptos que conforman el triángulo CID, se establece a continuación una breve descripción de cada uno de ellos:

La confidencialidad se refiere a la protección de la información, en cualquiera de sus estados, ya sea en el procesamiento, transporte, o almacenamiento, de no estar disponible a cualquier persona u organización no autorizada por su propietario o dueño de datos.

La integridad es la capacidad de asegurar que la información es exacta y precisa en el almacenamiento, transporte; que es y ha sido procesada correctamente y que no ha sido modificada en ninguna manera no autorizada. Los controles de integridad tienen que estar incluidos en el nivel de procesamiento para reducir los riesgos de error humano, así como del robo o fraude.

La disponibilidad busca asegurar que la información está asequible de manera oportuna, pero únicamente para aquellos usuarios que son autorizados de tenerla, estableciendo cuándo y en dónde deben tenerla.

Previo a establecer los requerimientos de seguridad, es necesario analizar el proceso para el desarrollo de un Sistema de Gestión de Seguridad de la Informacion SGSI, que está basado en la norma ISO/IEC 27001, para que exista concordancia en el desarrollo de este proyecto, dicho proceso se describe en la Figura 4.

Se ha descrito con anterioridad la misión, visión, los objetivos de la empresa, los productos o servicios, a continuación se detallarán los procesos que sustentan la entrega de el/los productos o servicios y los recursos necesarios para el cumplimiento de dichos procesos.

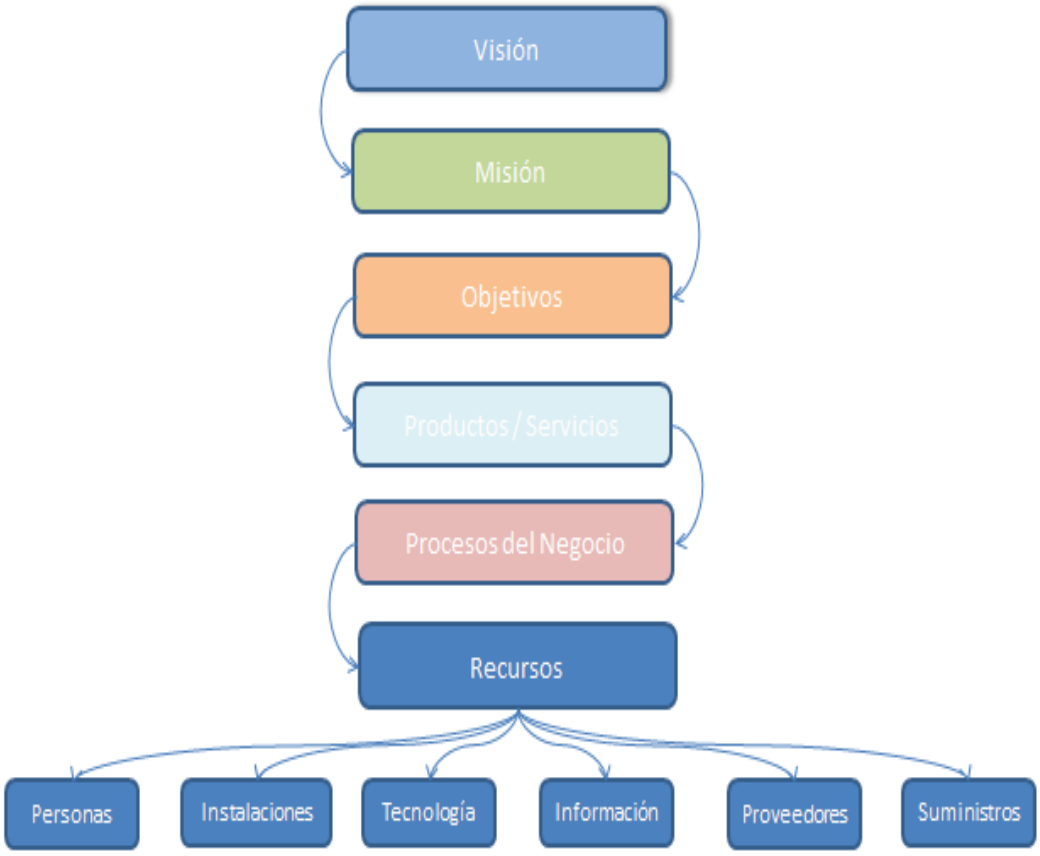


Figura 4. Alcance del SGSI
Fuente: NORMA ISO/IEC 27001
Elaborado por el autor

1.4.2.1 Procesos del Negocio

Son los procesos que sustentan la entrega de los productos o servicios clave de la empresa, en este caso KUEHNE+NAGEL división PERECIBLES, tal y como sugiere el desarrollo del Sistema de Gestión de la Seguridad de la Información SGSI.

Luego de las entrevistas realizadas en la empresa, se llegó a determinar la cadena de valor, esbozada en la Figura 5, en la cual hay tres grandes procesos en los que la empresa se enfoca.

De esos procesos, se escogió el proceso "Planificación y Programación" ya que es el que contiene los subprocesos más críticos, los mismos que se desarrollan dentro de las instalaciones de la empresa.

Figura 5. Cadena de valor KUEHNE-NAGEL división PERECIBLES.
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

El proceso PLANIFICACIÓN Y PROGRAMACIÓN contiene, a su vez, los subprocesos que se detallan en la Figura 6.

Para el cumplimiento de las etapas del PLANIFICACIÓN Y PROGRAMACIÓN, se utilizan recursos como personas, instalaciones, información, proveedores, recursos, tecnología.

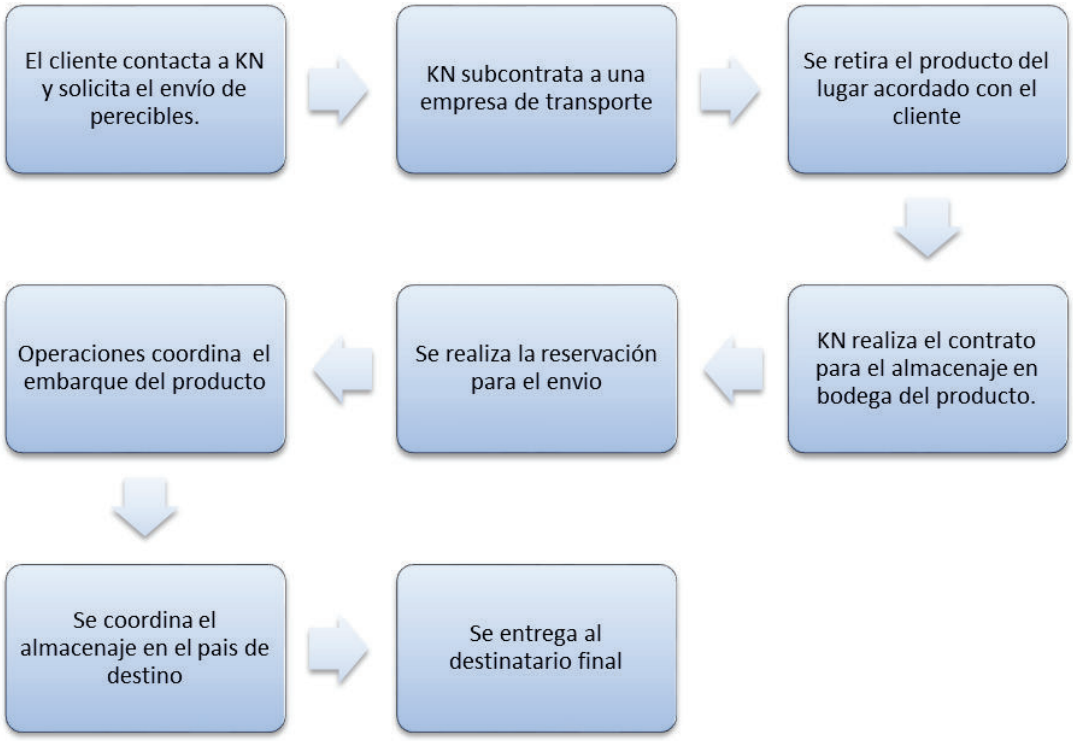


Figura 6. Subprocesos de Planificación y Programación.
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

La norma ISO/IEC 27001 propone gestionar los riesgos de la información utilizando normas internacionales tales como MAGERIT, ISO/IEC 27005, entre otras igualmente aceptadas.

Para esta etapa del proyecto se utilizará ISO 27005, la cual ha nacido claramente para apoyar la tarea del análisis y la gestión de riesgos en el marco de un SGSI como se observa en la Figura 7.

Esta 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

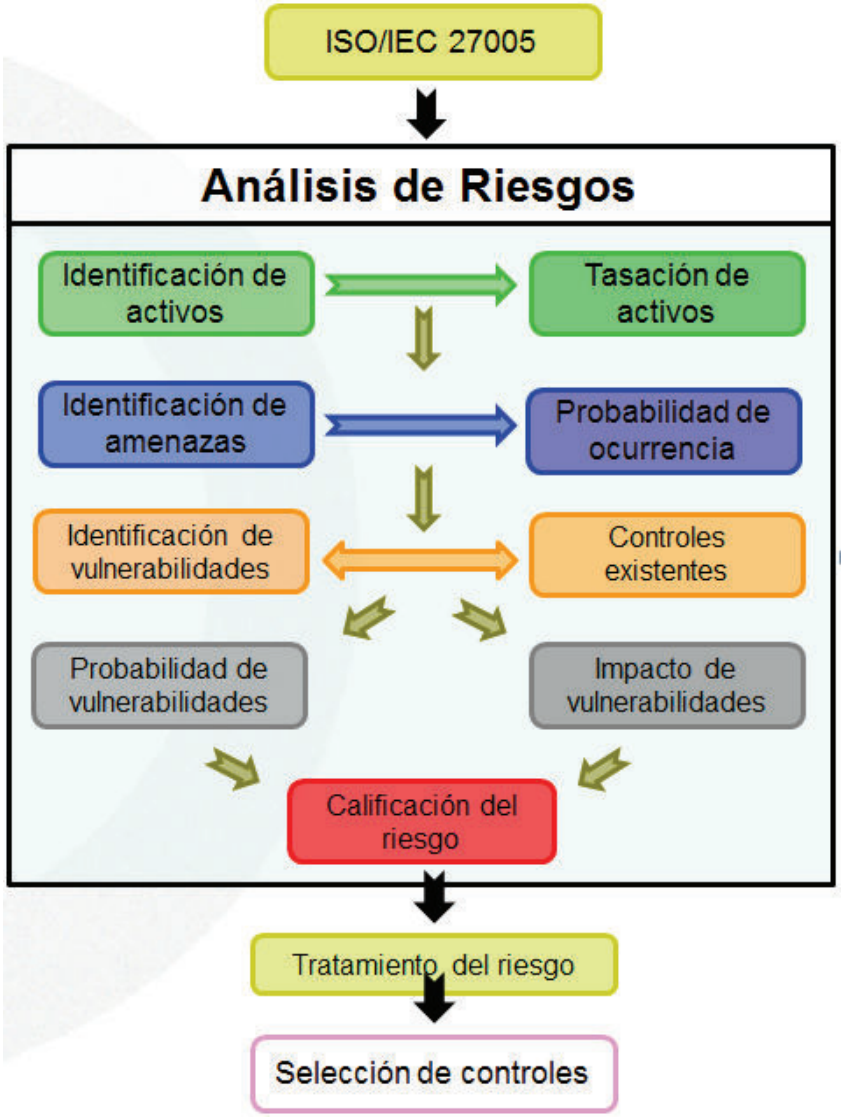


Figura 7. Proceso para determinación del riesgo y su gestión según ISO 27005.
Fuente: ISO/IEC 27005
Elaborado por el autor

1.4.2.2 Identificación de activos de información.

La Información debe ser considerada como un activo por lo que, al igual que otros activos importantes de la empresa, es esencial para el negocio de una organización y, en consecuencia, necesita estar protegida adecuadamente.

La información que maneja una empresa puede ser presentada de distintas formas, las más comunes se listan a continuación.

- Impresa / Escrita:
    - Formularios
    - Resoluciones
    - Actas
    - Informes

- Electrónica / Digital:
    - Correo electrónico, mensajería instantánea
    - Archivos ofimáticos y otros
    - Bases de datos, registros (Logs)

En las entrevistas desarrolladas en KUEHNE-NAGEL división PERECIBLES para la identificación de activos de información (inventario), se recopiló el siguiente listado de los atributos que permiten identificar plenamente a los activos:

Nombre del Activo: Identificador por el cual se va a reconocer al activo de información dentro del proceso, se utiliza un nombre particular y diferenciable.

Descripción del activo: Información adicional que permite concebir de manera única al activo de información. Además, permite determinar si el activo de información incluye otros activos. Por ejemplo, el activo “Información de contratos” puede contener: requerimientos, copias de documentos, etc.

Propietario/Dueño de datos: Persona responsable por el activo de información.

Localización: Indica donde se encuentra específicamente ubicado el activo, por ejemplo: archivadores, archivos de áreas, carpetas, escritorios, oficina, etc.

Contenedor: Medio (físico, lógico o magnético) donde se aloja la información electrónica:

- Aplicativo
- Base de datos
- Archivo (Word, excel, power point, txt, etc.)

Correo
Servidor/Computador/Portable/Tablet
Dispositivo externo (Cd/DVD, USB, etc.)
Unidad de respaldo (Cinta, disco magnético, la nube, etc.)

La norma ISO/IEC 27001:2013 recomienda no hacer una estimación de todos los activos de la organización ya que, en primer lugar, ciertos activos no aportarían un valor informativo fundamental para el desarrollo del proyecto y, en segundo lugar, complica el cumplimiento de plazos. Lo recomendable es elegir un grupo de activos reducido pero significativo para la empresa, es así que, conjuntamente con personal de KUEHNE+NAGEL división PERECIBLES, se llegó a determinar que los activos que participan en estos procesos son los que se encuentran descritos en la Tabla 8.

Clasificación	Activos	Propietario/Dueños del activo	Localización	Contenedor
Activos Físicos	Servidores	Infraestructura/TI	Rack de comunicaciones	N/A
	Computadores	Infraestructura/TI	Puesto determinado para el usuario	N/A
	Teléfonos	Infraestructura/TI	Puesto determinado para el usuario	N/A
	Impresoras	Infraestructura/TI	Oficina KUEHNE+NAGEL división PERECIBLES	N/A
	Switches	Infraestructura/TI	Rack de comunicaciones	N/A
	Router	Infraestructura/TI	Rack de comunicaciones	N/A
	Instalaciones (Oficina)	N/A	KUEHNE+NAGEL división PERECIBLES	N/A
Procesos / Activos de servicios de TI	Aplicación web de facturación	KUEHNE+NAGEL	Sitio Remoto KN	Servidores, Base de datos
	Aplicación web de manejo de reservaciones	KUEHNE+NAGEL	Sitio Remoto KN	Servidores, Base de datos

Información	Información de clientes	Dep. de Coordinación	Computadores	Archivos, correo
	Información de proveedores	Dep. de Coordinación	Computadores	Archivos, correo
	Guías de envío	Dep. de Coordinación	Computadores	Archivos, correo
	Correo Electrónico	Usuario	Computadores	Computador
	Sistema Operativo	Infraestructura/TI	Computadores	Computador
Recursos humanos	Personal de Coordinación	N/A	KUEHNE+NAGEL división PERECIBLES	N/A
	Personal de Operaciones	N/A	KUEHNE+NAGEL división PERECIBLES	N/A
	Proveedores	N/A	Externos	N/A

Tabla 8. Clasificación de activos de información.
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

1.4.2.3 Ponderación de la criticidad de activos.

La ponderación de activos es una etapa en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

Esta ponderación fue realizada en términos de “alto, medio o bajo” donde se asigna un valor cuantitativo a cada valor cualitativo, como se muestra en la Tabla 9, lo cual es una buena práctica ya que encasilla las respuesta dentro de un rango controlado, permitiendo a los encuestados responder rápidamente y con veracidad.

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Tabla 9. Valoración de los activos.
Elaborado por el autor

1.4.2.4 Tasación de activos

La valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estos son los ejes en los que se basa la seguridad de la información. En algunos casos, se utiliza el término “no aplica” ya que el activo no puede ser calificado bajo ninguno de los conceptos CID.

La Tabla 10 contiene el inventario de activos de información levantados durante la entrevista realizada, se incluye la tasación; el valor de tasación es el promedio de los campos “Criterios de Tasación”. Ver Anexo 2.

Activos	Criterios de Tasación			Tasación
	Confidencialidad	Integridad	Disponibilidad	
Servidores	2	3	3	2,667
Computadores	2	3	3	2,667
Teléfonos	1	1	2	1,333
Switches	2	3	3	2,667
Router	2	3	3	2,667
Impresoras	1	1	2	1,333
Instalaciones	No aplica	No aplica	3	3,000
Aplicación web de facturación	3	3	3	3,000
Aplicativo de manejo de reservaciones	3	3	3	3,000
Información de clientes	3	2	2	2,333
Información de proveedores	2	2	3	2,333
Guías de envío	3	3	1	2,333
Correo Electrónico	3	3	2	2,667
Sistema Operativo	2	3	2	2,333
Personal de Coordinación	No aplica	No aplica	2	2,000
Personal de Operaciones	No aplica	No aplica	2	2,000
Proveedores	No aplica	No aplica	2	2,000

Tabla 10. Tasación de activos.
Elaborado por el autor

Conjuntamente con el personal de KUEHNE+NAGEL división PERECIBLES, se determinó que los activos de información cuya valoración resultó ser mayor de dos (2), serán los que nos servirán en procesos siguientes, es decir identificar las amenazas. La norma ISO/IEC 27001:2013 no determina qué valor establecer como parámetros, pero hace una recomendación acerca de separar los activos críticos de los menos críticos.

1.4.2.5 Identificación de amenazas a los activos de información.

Una amenaza es cualquier causa que pueda infligir daño a un sistema u organización. Un ejemplo real de amenaza es un virus informático el cual va ligado directamente a explotar una vulnerabilidad típica que es la falta de software antivirus, el término vulnerabilidad y su tratamiento se puntualizará posteriormente.

Las amenazas pueden ser clasificadas como:

- ✓ Naturales
- ✓ Tecnológicas
- ✓ Fallas Humanas intencionales
- ✓ Fallas Humanas no intencionales

Se recuerda que se ha trabajado sólo con los activos con criticidad mayor a 2 de la Tabla 10, debido a que ese es el objetivo principal de hacer la tasación.

En el Anexo 3, se encuentra un listado de amenazas y vulnerabilidad las cuales pueden servir como guía para la determinación de las mismas.

En la Tabla 11, se muestra el listado de las amenazas que están sujetos los activos de información, el listado de dichas amenazas fue realizado conjuntamente con el personal de la empresa.

Activos	Amenazas
Servidores	• Desconexión de la red • Código malicioso (virus, troyanos, etc.) • Falla / Daño del equipo • Acceso físico no autorizado • Falla de suministro de energía
Computadores	• Desconexión de la red • Falla / Daño del equipo • Acceso físico no autorizado
Switches	• Falla / Daño del equipo • Código malicioso (virus, troyanos, etc.) • Falla de suministro de energía • Acceso físico no autorizado
Router	• Falla / Daño del equipo • Código malicioso (virus, troyanos, etc.) • Falla de suministro de energía • Acceso físico no autorizado
Instalaciones	• Incendio • Falla suministro energía eléctrica
Aplicación web de facturación	• Interrupción del servicio • Modificación, eliminación de datos por usuario autorizado y/o no autorizado
Aplicativo de manejo de reservaciones	• Interrupción del servicio • Modificación, eliminación de datos por usuario autorizado y/o no autorizado

Información de clientes	• Pérdida de información electrónica • Corrupción de la información
Información de proveedores	• Pérdida de información electrónica • Corrupción de la información
Guías de envío	• Pérdida de la guía • Corrupción del documento
Correo Electrónico	• Imposibilidad de descargar o enviar correo • Corrupción del archivo .pst
Sistema Operativo	• Código malicioso (virus, troyanos, etc.)

Tabla 11. Amenazas para los activos.
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

1.4.2.6 Ponderación del Impacto de materializarse la amenaza.

La ponderación se la realizó conjuntamente con personal de KUEHNE+NAGEL división PERECIBLES tomando en cuenta el impacto financiero e institucional, es decir, en esta escala si una amenaza es calificada como tres (3), significa que se podría afectar de forma crítica a la empresa, por ejemplo, perdiendo contratos lo cual implica pérdidas económicas; así mismo, si una amenaza es calificada como uno (1), se entiende que el negocio podrá seguir operando de una manera estable mientras se restablecen los procesos o servicios que fueron interrumpidos. Dicha ponderación se encuentra listada en la Tabla 12.

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Tabla 12. Ponderación del impacto de materializarse la amenaza
Elaborado por el autor

1.4.2.7 Identificación de vulnerabilidades

La vulnerabilidad es una debilidad en el sistema de seguridad de la información, la cual es una entrada para que una amenaza pueda o no materializarse, es decir que la vulnerabilidad en sí mismo no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza se concrete y afecte o haga daño.

De esta manera, los involucrados en la determinación de amenazas encuentran este proceso menos largo y complicado; si durante el transcurso del listado de las amenazas surgen otras, estas deben ser apuntadas para el posterior análisis y determinación si es o no una amenaza real hacia la seguridad de la información.

La Tabla 13, lista las distintas vulnerabilidades que se evidencian en los activos de la empresa.

Activos	**Amenazas**	**Vulnerabilidades**
Servidores	Desconexión de la red	Cableado estructurado deficiente.
	Código malicioso (virus,	No existe antivirus licenciado

Activos	Amenazas	Vulnerabilidades
	troyanos, etc.)	
	Falla / Daño del equipo	Falta de mantenimiento
	Acceso físico no autorizado	Control de acceso inadecuado.
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.
Computadores	Desconexión de la red	Cableado estructurado deficiente.
	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.
	Falla / Daño del equipo	Falta de mantenimiento
	Acceso físico no autorizado	Control de acceso inadecuado.
Switches	Falla / Daño del equipo	Falta de mantenimiento
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.
	Acceso físico no autorizado	Control de acceso inadecuado.
Router	Falla / Daño del equipo	Falta de mantenimiento
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.
	Acceso físico no autorizado	Control de acceso inadecuado.
Instalaciones	Incendio	Falta de sensores de incendio.

Activos	Amenazas	Vulnerabilidades
	Falla suministro energía eléctrica	Inexistencia de sistema de alimentación alterno
Aplicación web de facturación	Modificación, eliminación de datos por usuario autorizado y/o no autorizado	Falta capacitación
		Control de acceso inadecuado.
Aplicativo de manejo de reservaciones	Modificación, eliminación de datos por usuario autorizado y/o no autorizado	Falta capacitación
		Control de acceso inadecuado.
Información de clientes	Pérdida de información electrónica	Ausencia de política de respaldos.
	Corrupción de la información	No existe antivirus licenciado.
Información de proveedores	Pérdida de información electrónica	Ausencia de política de respaldos.
	Corrupción de la información	No existe antivirus licenciado.
Guías de envío	Pérdida de la guía	Ausencia de política de respaldos.
	Corrupción del documento	No existe antivirus licenciado.
Correo Electrónico	Imposibilidad de descargar o enviar correo.	No existe antivirus licenciado.
		Ausencia de política de respaldos.
Sistema Operativo	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.

Tabla 13. Vulnerabilidades encontradas.
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

1.4.2.8 Tasación de la probabilidad de que la amenaza explote la vulnerabilidad.

La calificación que se muestra en la Tabla 14 es, términos cuantitativos del 1 al 3, que tan probable es que una amenaza explote una o varias de las vulnerabilidades encontradas.

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Tabla 14. Tasación de la posibilidad que la amenaza explote la vulnerabilidad.
Elaborado por el autor

Luego de establecer y listar tanto las amenazas como las vulnerabilidades, la norma ISO/IEC 27005 recomienda hacer una calificación del riesgo y al mismo tiempo valorar cualitativamente la amenaza para analizar posteriormente los controles a implementar.

1.4.2.9 Análisis y Evaluación del Riesgo

La Tabla 15 muestra la calificación del riesgo, haciendo un análisis entre las amenazas y las vulnerabilidades encontradas, esta calificación del riesgo se la realiza haciendo una multiplicación de la probabilidad por el impacto (PxI).

Activos	Amenazas	Vulnerabilidades	Probabilidad amenaza explote vulnerabilidad	Impacto de materializarse la amenaza	Calificación del riesgo PxI
Servidores	Desconexión de la red	Cableado estructurado deficiente.	2	2	4
	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado	2	3	6
	Falla / Daño del equipo	Falta de mantenimiento	1	2	2
	Acceso físico no autorizado	Control de acceso inadecuado.	1	2	2
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	1	3	3
Computadores	Desconexión de la red	Cableado estructurado deficiente.	1	2	2
	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.	2	3	6

Activos	Amenazas	Vulnerabilidades	Probabilidad amenaza explote vulnerabilidad	Impacto de materializarse la amenaza	Calificación del riesgo Pxl
	Falla / Daño del equipo	Falta de mantenimiento	1	2	2
	Acceso físico no autorizado	Control de acceso inadecuado.	1	2	2
Switches	Falla / Daño del equipo	Falta de mantenimiento	1	3	3
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	1	3	3
	Acceso físico no autorizado	Control de acceso inadecuado.	1	2	2
Router	Falla / Daño del equipo	Falta de mantenimiento	1	3	3
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	1	3	3
	Acceso físico no autorizado	Control de acceso inadecuado.	1	2	2
Instalaciones	Incendio	Falta de sensores de incendio.	1	3	3
	Falla suministro energía eléctrica	Inexistencia de sistema de alimentación alterno	2	3	6

Activos	Amenazas	Vulnerabilidades	Probabilidad amenaza explote vulnerabilidad	Impacto de materializarse la amenaza	Calificación del riesgo Pxl
Aplicación web de facturación	Modificación, eliminación de datos por usuario autorizado y/o no autorizado	Falta capacitación	1	2	2
		Control de acceso inadecuado.	2	2	4
Aplicativo de manejo de reservaciones	Modificación, eliminación de datos por usuario autorizado y/o no autorizado	Falta capacitación	1	2	2
		Control de acceso Inadecuado.	2	2	4
Información de clientes	Pérdida de información electrónica	Ausencia de política de respaldos.	2	2	4
	Corrupción de la información	No existe antivirus licenciado.	2	2	4
Información de proveedores	Pérdida de información electrónica	Ausencia de política de respaldos.	2	2	4
	Corrupción de la información	No existe antivirus licenciado.	2	2	4
Guías de envío	Pérdida de la guía	Ausencia de política de respaldos.	2	2	4
	Corrupción del documento	No existe antivirus licenciado.	2	2	4

Activos	Amenazas	Vulnerabilidades	Probabilidad amenaza explote vulnerabilidad	Impacto de materializarse la amenaza	Calificación del riesgo Pxl
Correo Electrónico	Imposibilidad de descargar o enviar correo.	Ausencia de política de respaldos.	2	2	4
		No existe antivirus licenciado.	2	2	4
Sistema Operativo	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.	2	3	6

Tabla 15. Calificación del Riesgo
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

1.4.2.10 Plan de tratamiento del riesgo

Según la norma ISO/IEC 27005, el plan de tratamiento del riesgo se lo puede realizar de varias maneras como por ejemplo transferir el riesgo hacia terceros, aceptar el riesgo, reducir el riesgo o evitar el riesgo; para el presente proyecto la estrategia para manejo del riesgo considerará la reducción del mismo utilizando normas internacionales. La decisión para el manejo del riesgo no solo la debe tomar el departamento de Sistemas sino, es una decisión conjunta con unidades del negocio y la alta gerencia.

Esta decisión se toma una vez que se han estudiado los diferentes escenarios para una misma amenaza que explote una vulnerabilidad, la cual conlleve a un impacto negativo en la empresa. Por lo tanto, el nivel de aceptación del riesgo conlleva a la aplicación o no de procedimientos para mitigar amenazas, o contrarrestar sus efectos y probabilidad de que ocurra.

En la figura 8 se muestran 4 niveles de tolerancia del riesgo, tomando los valores de la Tabla 15, conjuntamente con personal de KUEHNE+NAGEL división PERECIBLES, se ha considerado que el riesgo intolerable o extremo, es decir el activo con calificación del riesgo de 2 o superior, será sobre el cual se aplicarán los controles.

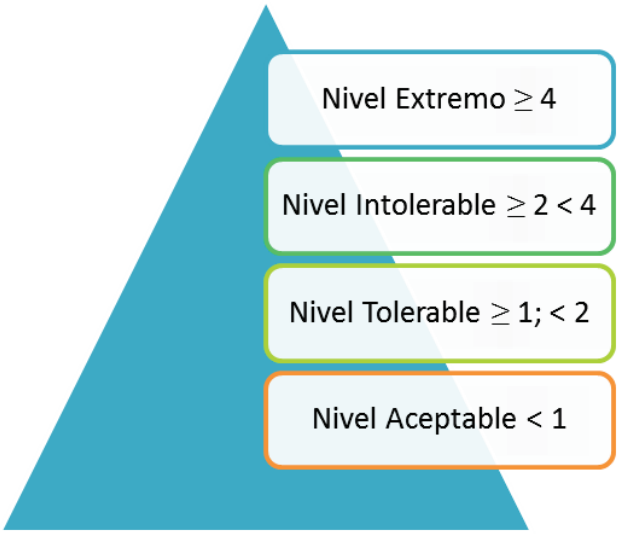


Figura 8. Nivel de aceptación del riesgo.
Elaborado por el autor

1.4.2.11 Selección de controles según la norma ISO/IEC 27002:2013

La norma ISO/IEC 27001:2013 recomienda utilizar cualquier norma para la mitigación de los riesgos encontrados, entre las normas más conocidas están NIST, COBIT y la norma ISO/IEC 27002:2013, esta última será la utilizada por su relación más directa con la norma ISO/IEC 27001:2013 que es la norma en la que se apoya este proyecto.

La nueva estructura de la ISO/IEC ISO 27002:2013 se muestra en la figura 9, tiene 14 dominios, 35 objetivos de control y 114 controles.

El listado completo de estos dominios objetivos de control y controles se encuentra en el Anexo 4.

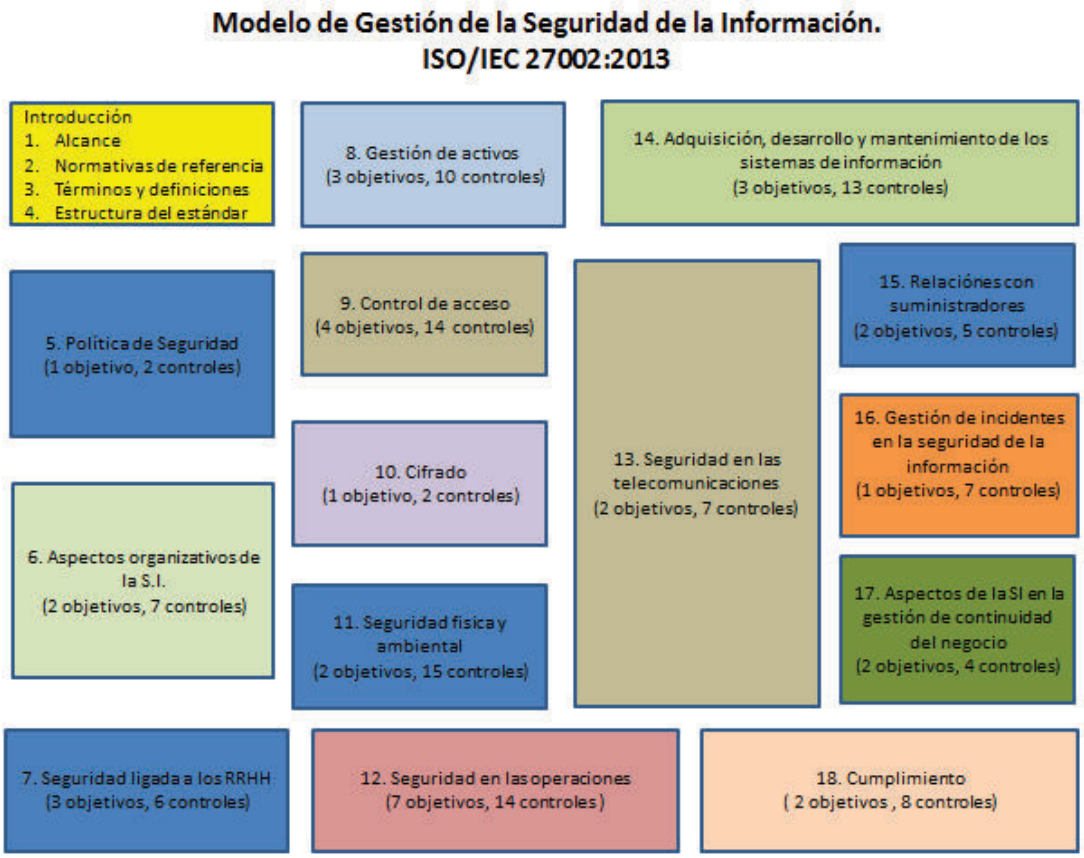


Figura 9. Modelo de Gestión ISO/IEC 27002:2013
Fuente: ISO/IEC 27002:2013
Elaborado por el autor

1.4.2.12 Implementación de Objetivos de control y controles según la norma ISO/IEC 27002:2013

En la Tabla 16 se detallan los objetivos de control y controles para mitigar los diferentes riesgos a los activos de la empresa KUEHNE+NAGEL división PERECIBLES, estos controles se encuentran detallados en el Anexo 3.

Activos	**Amenazas**	**Vulnerabilidades**	**Objetivos de control**		**Controles**	
Servidores	Desconexión de la red	Cableado estructurado deficiente.	11.2	Seguridad de los equipos	11.2.3	Seguridad del cableado
	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
	Falla / Daño del equipo	Falta de mantenimiento	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos
	Acceso físico no autorizado	Control de acceso inadecuado.	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos
			9.1	Requisitos de negocio para el control de accesos	9.1.1	Política de control de accesos
			9.2	Gestión de acceso de usuario	9.2.5	Revisión de los derechos de acceso a los usuarios

Activos	**Amenazas**	**Vulnerabilidades**	**Objetivos de control**		**Controles**	
			9.3	Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación
			11.1	Áreas Seguras	11.1.1	Perímetro de seguridad física
					11.1.2	Controles físicos de entrada
					11.1.3	Seguridad de oficinas, despachos y recursos
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	11.2	Seguridad de los equipos	11.2.2	Instalaciones de suministro
					11.2.3	Seguridad del cableado
Computadores	Desconexión de la red	Cableado estructurado deficiente.	11.2	Seguridad de los equipos	11.2.3	Seguridad del cableado
	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
	Falla / Daño del equipo	Falta de mantenimiento	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos
	Acceso físico no	Control de acceso	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos

Activos	**Amenazas**	**Vulnerabilidades**	**Objetivos de control**		**Controles**	
	autorizado	inadecuado.	9.2	Gestión de acceso de usuario	9.2.5	Revisión de los derechos de acceso a los usuarios
Switches	Falla / Daño del equipo	Falta de mantenimiento	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	11.2	Seguridad de los equipos	11.2.2	Instalaciones de suministro
					11.2.3	Seguridad del cableado
	Acceso físico no autorizado	Control de acceso inadecuado.	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos
			9.1	Requisitos de negocio para el control de accesos	9.1.1	Política de control de accesos
			9.2	Gestión de acceso de usuario	9.2.5	Revisión de los derechos de acceso a los usuarios
			9.3	Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación
Router	Falla / Daño del equipo	Falta de mantenimiento	11.2	Seguridad de los equipos	11.2.4	Mantenimiento de los equipos

Activos	**Amenazas**	**Vulnerabilidades**	**Objetivos de control**		**Controles**	
	Falla de suministro de energía	Inexistencia de sistema de alimentación alterno.	11.2	Seguridad de los equipos	11.2.2	Instalaciones de suministro
					11.2.3	Seguridad del cableado
	Acceso físico no autorizado	Control de acceso inadecuado.	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos
			9.1	Requisitos de negocio para el control de accesos	9.1.1	Política de control de accesos
			9.2	Gestión de acceso de usuario	9.2.5	Revisión de los derechos de acceso a los usuarios
			9.3	Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación
Instalaciones	Incendio	Falta de sensores de incendio.	11.1	Áreas Seguras	11.1.4	Protección contra las amenazas externas y ambientales
	Falla suministro energía eléctrica	Inexistencia de sistema de alimentación alterno	11.2	Seguridad de los equipos	11.2.2	Instalaciones de suministro
Aplicación web de	Modificación, eliminación de datos	Falta capacitación	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos

Activos	**Amenazas**	**Vulnerabilidades**	**Objetivos de control**		**Controles**	
facturación	por usuario autorizado y/o no autorizado	Control de acceso inadecuado.	9.3	Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación
			9.4	Control del acceso a sistemas y aplicaciones	9.4.1	Restricción del acceso a la información
					9.4.3	Gestión de contraseñas de usuario
Aplicativo de manejo de reservaciones	Modificación, eliminación de datos por usuario autorizado y/o no autorizado	Falta capacitación	8.1	Responsabilidad sobre los activos	8.1.3	Uso aceptable de los activos
		Control de acceso inadecuado.	9.3	Responsabilidades del usuario	9.3.1	Uso de información confidencial para la autenticación
			9.4	Control del acceso a sistemas y aplicaciones	9.4.1	Restricción del acceso a la información
					9.4.3	Gestión de contraseñas de usuario
Información de clientes	Pérdida de información electrónica	Ausencia de política de respaldos.	12.3	Copias de seguridad	12.3.1	Copias de seguridad de la información
	Corrupción de la información	No existe antivirus licenciado.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso

Activos	Amenazas	Vulnerabilidades	Objetivos de control		Controles	
Información de proveedores	Pérdida de información electrónica	Ausencia de política de respaldos.	12.3	Copias de seguridad	12.3.1	Copias de seguridad de la información
	Corrupción de la información	No existe antivirus licenciado.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
Guías de envío	Pérdida de la guía	Ausencia de política de respaldos.	12.3	Copias de seguridad	12.3.1	Copias de seguridad de la información
	Corrupción del documento	No existe antivirus licenciado.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
Correo Electrónico	Imposibilidad de descargar o enviar correo.	No existe antivirus licenciado.	12.3	Copias de seguridad	12.3.1	Copias de seguridad de la información
		Ausencia de política de respaldos.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso
Sistema Operativo	Código malicioso (virus, troyanos, etc.)	No existe antivirus licenciado.	12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso

Tabla 16. Selección de objetivos de control y controles
Fuente: ISO/IEC 27002:2013
Elaborado por el autor

De manera general, las empresas deberían definir un conjunto de políticas para la seguridad de la información, este objetivo se lo nombre explícitamente con el objetivo de control 5: Políticas de Seguridad y el control 5.1.1 “Conjunto de políticas para la seguridad de la información”, dicho objetivo de control y control elegido, no fueron incluidos en la Tabla 16 y se encuentran detallados en el Anexo 4.

Este control escogido sugiere a las empresas elaborar un conjunto de políticas para la seguridad de la información el cual debería ser definido, aprobado, publicado y comunicado a los usuarios y a las personas involucradas en todos los procesos del negocio.

1.4.2.13 Matriz de asociación de responsabilidades RACI

La matriz RACI es una matriz del tipo informativa, utilizada generalmente en el manejo de gestión de proyectos, la cual es útil para la asignación de roles y responsabilidades a un proyecto, se utiliza esta matriz por su versatilidad, de modo que se alineará los controles a implantar según la norma ISO/IEC 27002:2013. Ver Tabla 17.

Los roles están identificados como R, A, C, I significando:

- Responsible (Responsable): este rol tiene la responsabilidad mayor para la ejecución de las actividades en esta sección.
- Accountable (Quien rinde las cuentas): Este rol es el llamado a rendir cuentas si los riesgos se materializan (generalmente porque los controles preventivos fallan); por lo general es el responsable del presupuesto.
- Consulted (Consultado): Este es un rol de poca o nula intervención, que ofrece orientación y dirección a los involucrados más activamente.
- Informed (Informed): Este rol se debe mantener en contacto con el desarrollo de las actividades y los resultados de la ejecución de la tarea.

En relación con lo detallado en el punto 1.2.2, dentro de la empresa KUEHNE+NAGEL división PERECIBLES existen tres departamentos que son operaciones, coordinación, atención al cliente, junto con representantes de estas tres áreas o unidades de negocio, además del Departamento de Sistemas, se esbozó un matriz RACI preliminar de manera que se asienten las ideas acerca de roles y responsabilidades para el cumplimiento de implantación de controles descritos en la Tabla 16.

La matriz RACI puede ser muy simple o muy complicada dependiendo de los niveles del organigrama que la empresa haya realizado, los controles a implementar, entre otros; esta matriz es una herramienta para ayudar a determinar y describir quién hace qué en relación con el Sistema de Gestión de Seguridad de la Información, se puede añadir, cambiar o suprimir roles.

ISO/IEC 27002:2013 R = Responsible A = Accountable C = Consulted I = Informed		Usuarios	Gerente operativo	Depar. de Sistemas	Jefe Depar. Coordinac.	Jefe Depar. Operaciones
5. Políticas de Seguridad						
5.1.1	Conjunto de Políticas para la seguridad de la información.	I	A	R	C	C
8. Gestión de Activos						
8.1.3	Uso aceptable de los activos	I	A	R	C	C
9. Control de Acceso						
9.1.1	Política de control de accesos	I	A	R	C	C
9.2.5	Revisión de los derechos de acceso de los usuarios	I	A	R	C	C
9.3.1	Uso de información confidencial para la autenticación.	I	A	R		

ISO/IEC 27002:2013 R = Responsible A = Accountable C = Consulted I = Informed		Usuarios	Gerente operativo	Depar. de Sistemas	Jefe Depar. Coordinac.	Jefe Depar. Operaciones
9.4.1	Restricción del acceso a la información.	I	A	R		
9.4.3	Gestión de contraseñas de usuario	I	A	R		
11. Seguridad Física y Ambiental						
11.1.1	Perímetro de seguridad física.	I	A	R		
11.1.2	Controles físicos de entrada	I	A	R		
11.1.4	Protección contra las amenazas externas y ambientales	I	A	R		
11.2.2	Instalaciones de suministro		A	R		
11.2.3	Seguridad del cableado		A	R		
11.2.4	Mantenimiento de los equipos		A	R		
12. Seguridad en la Operativa						

ISO/IEC 27002:2013 R = Responsible A = Accountable C = Consulted I = Informed		Usuarios	Gerente operativo	Depar. de Sistemas	Jefe Depar. Coordinac.	Jefe Depar. Operaciones
12.2.1	Controles contra el código malicioso	I	A	R		
12.3.1	Copias de seguridad de la información.	I	A	R		

Tabla 17. Matriz RACI de roles y responsabilidades.
Elaborado por el autor

1.4.3 REQUERIMIENTOS DE COMUNICACIÓN

La determinación del tráfico que circulará por la red permitirá evitar cuellos de botella, congestionamiento en la red y asegurar la disponibilidad de los diferentes servicios de la red.

La estimación del tráfico se calculará a través de datos proporcionados por el departamento de sistema de TI de la empresa KUEHNE+NAGEL división PERECIBLES.

Actualmente la empresa cuenta con un enlace de 2 Mbps, busca determinar si se esté ancho de bando es suficiente para proporcionar los servicios de Internet, descarga de correo y además en nuevo servicio de voz sobre IP, asegurando su calidad y disponibilidad.

Los servicios que accederán a Internet serán:

- Acceso Web
    - Aplicaciones Web de reservaciones
    - Aplicaciones web de facturación.
    - Navegación Web
- Correo electrónico
- Telefonía.

Acceso a Web.

Tomando en cuenta que actualmente las personas no tienen ninguna restricción para el uso de Internet, se confía plenamente en su buen criterio para el uso de este servicio.

Para el cálculo del ancho de banda necesario para la navegación Web, el departamento de Sistema de la empresa no cuenta con dicha información por lo

que el cálculo será realizado con valores promedio, es así como, se considerará que los usuarios abren un promedio de 10 páginas web por hora. Teniendo en cuenta que el tamaño promedio de una página web es de 350 KB[8], se calcula:

$$\text{Carga acceso pagina web} = \frac{350\ \text{KB}}{1\ \text{pag web}} * \frac{10\ \text{pag web}}{1\ \text{hora}} * \frac{1\ \text{hora}}{3600\ \text{s}} * \frac{8\ \text{bits}}{1\ \text{Byte}}$$

$$\text{Carga acceso internet} = 7.78\ \text{Kbps}$$

Correo electrónico

La información proporcionada por el Departamento de Sistemas de la empresa es que los usuarios reciben un promedio de 5 correos por hora. Cada correo electrónico con un peso promedio de 200 KB por lo que la ecuación se utilizará esta información para el cálculo real del ancho de banda requerido para el uso óptimo del correo electrónico.

$$\text{Carga correo electronico} = \frac{200\ \text{KBytes}}{1\ \text{correo electr.}} * \frac{5\ \text{correos.}}{1\text{hora}} * \frac{1\ \text{hora}}{3600\ \text{s}} * \frac{8\ \text{bits}}{1\ \text{byte}}$$

$$\text{Tráfico correo electrónico} = 2.22\ \text{Kbps}.$$

Descarga de archivos

El operador de las aplicaciones de manejo de reservaciones o facturación, luego de generar el documento en línea puede descargar tanto la reserva como la factura, estos archivos pueden llegar a pesar 150 KB cada uno y se ha comprobado que el usuario podría descargar hasta 5 archivos.

[8]https://developers.google.com/speed/articles/web-metrics?hl=es-ES

$$\text{Carga descarga de archivos} = \frac{150\text{KB}}{1\text{ hora}} * \frac{5\text{ descargas}}{1\text{hora}} * \frac{1\text{ hora}}{3600\text{ s}} * \frac{8\text{ bits}}{1\text{ byte}}$$

$$\text{Carga descarga de archivos} = 1.66\text{ Kbps}$$

Estos valores establecidos nos servirán posteriormente para el cálculo del ancho de banda requerido para la empresa.

	Servicios	Ancho de banda Requerido por aplicación (Kbps)	Número de usuarios[9] (Kbps)	Ancho de banda total (Kbps)
KUEHNE+NAGEL división PERECIBLES	Correo Electrónico	2,22	50	111
	Acceso a Internet	7,77	50	389
	Descarga de archivos	1,66	50	83

Tabla 18. Ancho de banda requerido - KUEHNE+NAGEL división PERECIBLES
Elaborado por el autor

El ancho de banda necesario para brindar los servicios anteriormente descritos es la suma de los anchos de banda individuales.

$$\text{Ancho de banda total} = 111\text{ Kbps} + 389\text{ kbps} + 83\text{ kbps}$$

$$\text{Ancho de banda total} = 583\text{ kbps}$$

Capacidad para la red convergente

El concepto de red convergente implica la necesidad de transportar datos, voz y video sobre la misma red corporativa sin perjudicar el rendimiento de la misma;

[9]Información proporcionada por KUEHNE NAGEL EC

para lograr este propósito se realizará un cálculo estimado de cuánto ancho de banda se requiere y el número adecuado de enlaces de voz que serán requeridos para la implantación, sin dejar de lado la calidad de voz, latencia, perdida de paquetes, y seguridad de la transmisión.

Para el cálculo del tráfico telefónico se deberá tomar en cuenta tanto el ancho de banda requerido para una llamada utilizando el servicio de telefonía IP así como el número de conversaciones simultaneas que realiza la empresa KUEHNE+NAGEL división PERECIBLES durante un lapso de tiempo. Además, de los factores mencionada el cálculo del dimensionamiento del el tráfico de telefonía IP depende de factores como codec o codificador utilizar, tamaño del paquete de datos de voz, compresión en la cabecera RTP, supresión de silencio.

Según el códec empleado se utilizará más o menos ancho de banda y esto generalmente viene de la mano con la calidad de los datos transmitidos. En la Tabla 19 se listan los códecs más utilizados en la transmisión de voz sobre IP y sus principales características.

CODEC	CALIDAD DE AUDIO	Paquetes por segundo (PPS)	Ancho de banda requerido (Kbps)
G711	Buena	50	87.2
G722	Muy Buena	50	87.2
G723	Aceptable	33.3	21.9
G729	Promedio	50	31.2

Tabla 19. Codecs de voz más comunes usados en Telefonía IP[10].
Fuente: Tesis EPN "DISEÑO DE LA RED DE CORPORATIVA DE VOZ Y DATOS PARA EL SERVICIO ECUATORIANO DE CAPACITACION PROFESIONAL"
Elaborado por el autor

[10]http://www.3cx.es/ancho-de-banda-voip/

El códec elegido para el proyecto es el G.729 ya que brinda una buena calidad de voz y ancho de banda relativamente bajo.

En la Tabla 20, se detallan el volumen de llamadas y duración de las mismas. Estos valores fueron proporcionados por el departamento de sistemas de la empresa KUEHNE+NAGEL división PERECIBLES.

Localidad	Número de Llamadas por hora	Duración promedio de las llamadas (min)
KUEHNE+NAGEL división PERECIBLES	15	5

Tabla 20. Número de llamadas por hora y duración promedio de las llamadas
Fuente: Empresa Kuehne+Nagel UIO
Elaborado por el autor

Con los valores de la Tabla 19, se calcula el tráfico se utilizó la ecuación de Erlang, así:

$$A = \frac{H * Y}{T}$$

Donde:

A: Tráfico de Erlang

H: Tiempo promedio de uso de la línea.

Y: Número de llamadas un período de tiempo

Cuando H está en horas el valor de T es 1, si H está en minutos el valor de T es 60.

$$A = \frac{15 \text{ llamadas}}{1 \text{ hora}} * \frac{1 \text{ hora}}{60 \text{ minutos}} * 5 \text{ minutos}$$

$$A = 1{,}25 \text{ Erlang}$$

Está disponible en la Web una aplicación llamada “calculadora Erlangs and VoIP Bandwidth”[11], con la cual es posible averiguar el ancho de banda requerido, considerando ciertos parámetros que se describen brevemente a continuación.

- Algoritmo de codificación (codingalgorithm): es el algoritmo que se seleccionó haciendo el análisis con los datos de la Tabla 19.
- Duración de paquete (packet duration): 20 milisegundos.
- BHT (BusyHourTraffic): valor calculado con la ecuación de erlang.
- Porcentaje de bloqueo de llamadas: valor por defecto es 0.01

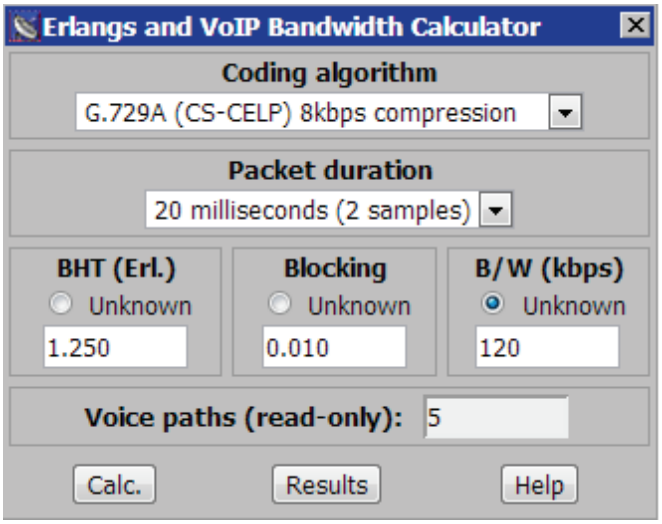


Figura 10. Resultado Cálculo Erlangs

Por lo tanto el ancho de banda requerido para el tráfico de voz en KUEHNE+NAGEL división PERECIBLES es de 120 kbps.

Localidad	Tráfico de voz (kbps)	Tráfico de Internet (kbps)	Tráfico total (kbps)
KUEHNE+NAGEL división PERECIBLES	120	583	703

Tabla 21. Ancho de banda de la red convergente
Elaborado por el autor

[11] http://www.erlang.com/calculator/eipb/

En la Tabla 21, se demuestra el valor del tráfico total proyectado para la red convergente, por lo tanto, de los resultados obtenidos se obtiene que el ancho de banda mínimo requerido para brindar el servicio de voz sobre IP, está satisfecho por el ancho de banda contratado actualmente el cual es de 2 Mbps.

Finalmente, después de haber descrito en detalle los requerimientos físicos, de seguridad de información y de comunicación en los puntos 1.4.1, 1.4.2 y 1.4.3 respectivamente se tiene un visión más clara de las siguientes etapas de este proyecto, principalmente del enfoque de seguridad que se utilizará para solventar dichos requerimientos.

2. CAPITULO 2

DISEÑO DE LA RED CORPORATIVA

2.1 INTRODUCCIÓN

Este capítulo tiene como objetivo el diseño de la red corporativa segura, eficiente, disponible y fortalecida que integre datos y voz de la empresa "KUEHNE+NAGEL división PERECIBLES", basándonos en el análisis de la situación actual y en el análisis de requerimientos realizados en el capítulo anterior.

El diseño de la red debe cubrir con solvencia los requerimientos y proyectar soluciones a mediano plazo para la corporación, esto se logra siguiendo las mejores prácticas, lineamientos y conceptos descritos en metodologías mundialmente aceptadas e implementadas con gran éxito como es el caso de la arquitectura modular SAFE de Cisco, la misma que brinda una metodología para el diseño e implementación de redes seguras empresariales, la cual es totalmente escalable, es decir permite ser usada tanto en redes pequeñas como en redes grandes.

En la última parte de este capítulo se realiza el dimensionamiento de los equipos de comunicación necesarios para la red, así como varias soluciones de seguridad de la información como respuesta al análisis de requerimientos en ese tema.

2.2 METODOLOGÍA DE DISEÑO

Existen varias arquitecturas, metodologías de diseño, normas aceptadas mundialmente, este proyecto se apoyará en la norma SAFE CISCO ya que esta norma ofrece información sobre las mejores prácticas para el diseño e implementación de redes enfocándose principalmente en la seguridad de la información.

De acuerdo con la norma ISO 27002:2013, existe un objetivo primordial para las organizaciones el cual es el de asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura, este objetivo está cubierto por el Dominio “13. Seguridad en las telecomunicaciones”. Ver Anexo 4.

La gestión adecuada y segura de las redes de información, requiere de la consideración del flujo de datos e información, implicaciones legales, monitoreo y protección. La información, ya sea pública, de uso interno, restringida y confidencial que pasa a través de redes públicas suele requerir de controles específicos y/o adicionales de protección.

La norma SAFE CISCO entrega una guía para el cumplimiento del objetivo de control “13.1 Gestión de la seguridad en las redes” para garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

La tabla 22 muestra la relación de la norma ISO/IEC 27002:2013 y la metodología SAFE CISCO.

Seguridad en las telecomunicaciones	**Fundamentos de SAFE CISCO**
Controles de red	• Seguridad y mitigación de ataques. • Aplicación de seguridad a través de la infraestructura (no sólo en los dispositivos de seguridad especializados)
Mecanismos de seguridad asociados a los servicios de red.	• Autenticación y autorización de usuarios y administradores de los recursos críticos de la red

Segregación de red	• Diseño lógico modular de la red. • Separación de sistemas de información, usuarios y dispositivos de red.

Tabla 22 Alineación ISO 27002:2013 y SAFE CISCO
Fuente: ISO/IEC 27002:2013 – Metodología Safe Cisco
Elaborado por el autor

2.2.1 DESCRIPCIÓN DE SAFE CISCO

La arquitectura SAFE de Cisco es una arquitectura modular de seguridad que proporciona lineamientos para la seguridad de la red corporativa priorizando las áreas funcionales. Si bien es cierto esta arquitectura usa productos CISCO, esto no es determinante a la hora de escoger un fabricante sino más bien es una guía para elegir los dispositivos necesarios por función y características. Las versiones de esta metodología han cambiado en forma más que en fondo, es decir, los cambios están más relacionados con la evolución de las nuevas tecnologías de seguridad; el principio bajo el cual esta norma fue desarrollada, que es el de priorizar la seguridad y rendimiento de las redes, permanece a través de los años.

Hay que tener en claro que SAFE es una arquitectura de seguridad que brinda protección de adentro hacia afuera de la red, y viceversa, detectando posibles atacantes en el menor tiempo posible, y aislándolos, logrando que el efecto adverso que estos puedan causar en la red sea el menos negativo, al mismo tiempo que protege a los datos y a los usuarios. La red corporativa debe proporcionar todos los servicios que los usuarios esperan, en el tiempo que lo requieran. Se enfoca en las amenazas que puedan existir en cada módulo y la forma de mitigar el riesgo que estas amenazas puedan explotar, en lugar de simplemente de ubicar dispositivos como firewall y otras tecnologías.

El propósito de este diseño es establecer los elementos activos y pasivos de la red en áreas funcionales constituidas por diferentes módulos, tomando en cuenta lineamientos y funciones específicas, logrando así que en cada módulo se

establezca un conjunto de medidas de seguridad, sin depender de una tecnología en particular.

Para un mejor entendimiento, resulta conveniente plantear un diagrama esquemático en bloques de la Arquitectura SAFE CISCO como se observa en la Figura 11.

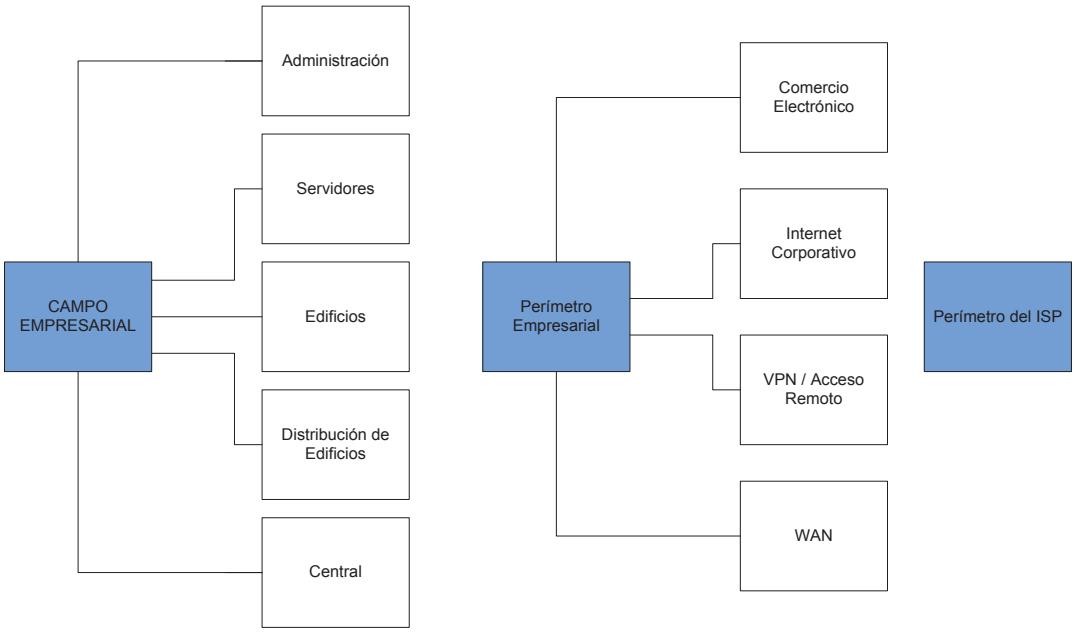


Figura 11. Estructura Modular SAFE CISCO
Fuente: Metodología SAFE CISCO
Elaborado por el autor

Para este proyecto se utilizará la guía para la implementación de SAFE CISCO para empresas medianas, que permitirá plantear el diseño de la red con la arquitectura original de SAFE CISCO con el fin de demostrar la gran escalabilidad de esta arquitectura.

La guía para empresas pequeñas y medianas determina 2 módulos diferenciados claramente así:

- Módulo de Internet Corporativo
- Módulo de Campus

- Perímetro de Proveedor de Servicios (SP)

Lógicamente, estos tres módulos se estructuran como se muestra en la Figura 12.

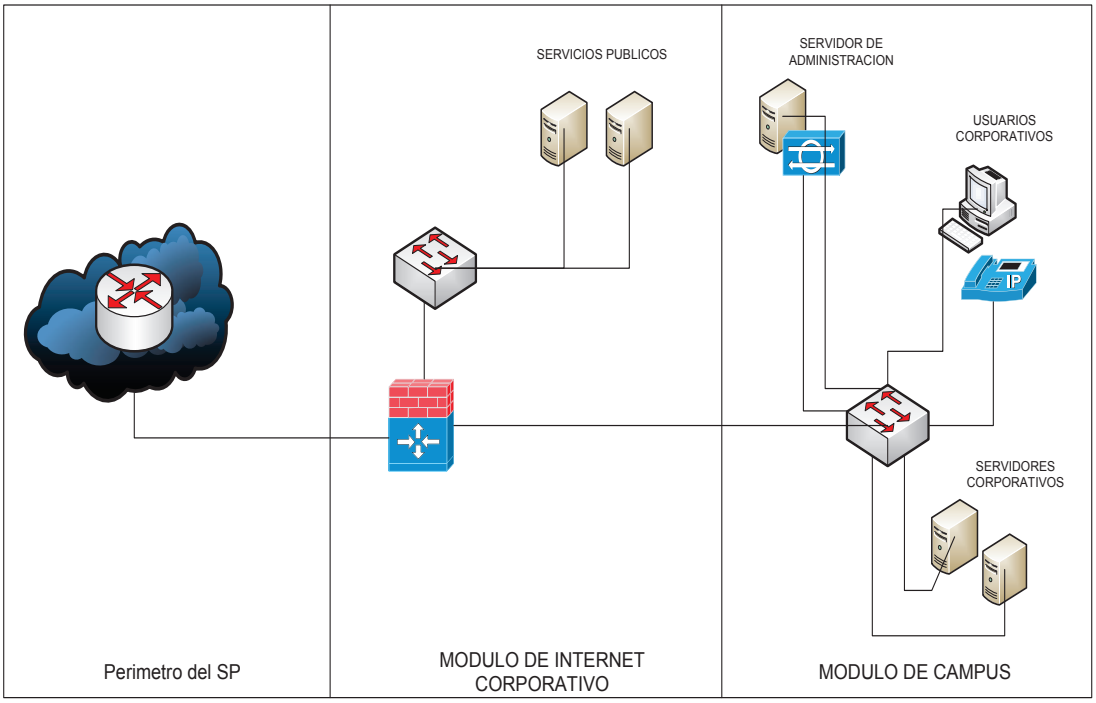


Figura 12. Diseño de seguridad SAFE para empresas pequeñas/medianas
Fuente: Metodología SAFE CISCO
Elaborado por el autor

2.2.1.1 Módulo de Campus

Este módulo está constituido por estaciones de trabajo de usuarios finales, teléfonos IP, servidores internos, switches capa 2, servidor de administración de ser el caso. Cabe puntualizar que si bien físicamente los servidores se encuentran en el mismo lugar, lógicamente éstos se encuentran separados.
Dichas soluciones podrán ser Virtualizados brindando las mismas funcionalidades como si fueran servidores físicos.

En la Tabla 23, se detallan los componentes que se incluyen en el Módulo de Campus y sus características principales.

Equipos	Características
Estaciones de trabajo	Proveen servicios a usuarios finales correctamente autenticados.
Switches capa 2	Proveen servicios de capa 2 a usuarios, con soporte para VLAN.
Servidores Internos	Proveen servicios como correo electrónico (pop3 y SMTP), impresión, entrega de archivos.

Tabla 23. Dispositivos en el módulo Campo
Fuente: Metodología SAFE CISCO
Elaborado por el autor

Amenazas a combatir

Las amenazas que busca combatir este módulo se encuentran esbozadas en la figura 13.

Figura 13. Amenazas a combatir en el módulo de Campo.
Fuente: Metodología SAFE CISCO
Elaborado por el autor

2.2.1.2 Módulo de Internet corporativo

Este módulo brinda a los usuarios de la red interna los servicios de Internet, de igual manera a los usuarios externos acceso a los servidores públicos que se encuentran en la Zona Desmilitarizada (DMZ).

En la Tabla 24, sólo se muestran los componentes principales que podrían ser incluidos en este módulo.

Equipos	**Características**
Servidor FTP / HTTP	Provee información pública acerca de la organización
Firewall o Router Firewall	Provee protección a nivel de red de los recursos de la organización, filtrado de tráfico, acceso VPN para usuarios remotos.
IDS / IPS	Sistemas de detección de intrusos / Sistema de prevención de intrusos
Switch capa 2	Asegura que el tráfico atraviese el firewall, con soporte para VLAN.

Tabla 24. Dispositivos en el módulo Internet Corporativo.
Fuente: Metodología SAFE CISCO
Elaborado por el autor

Implementar funcionalidad y seguridad es el reto para este módulo, considerando una empresa pequeña como esta, un Router con funcionalidad de firewall y VPN brinda una gran flexibilidad ya que soportará servicios avanzados como ruteo, Calidad de Servicio (Quality of service) QoS, soporte multiprotocolo, entre otros.

Amenazas a combatir

El módulo de Internet Corporativo debe ser considerado como un módulo perimetral, es decir que se enfoca en la protección de la empresa a nivel de todo el perímetro que la rodea. La figura 14 muestra las principales amenazas a combatir.

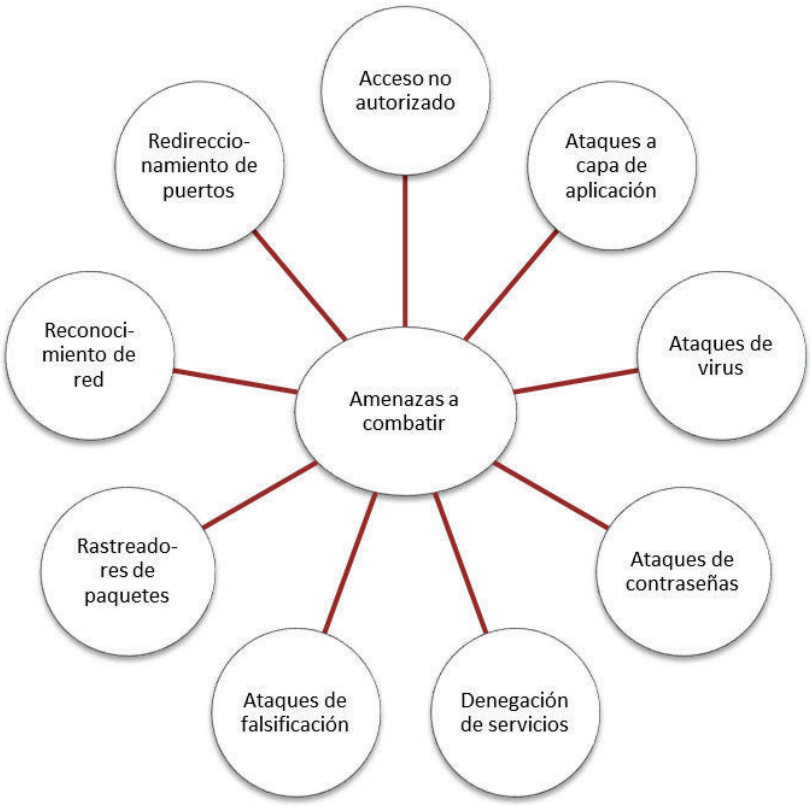


Figura 14. Amenazas a combatir en el módulo Internet Corporativo
Fuente: Metodología SAFE CISCO
Elaborado por el autor

2.3 DISEÑO DE LA RED

2.3.1 DISEÑO DE LA RED CORPORATIVA CONVERGENTE

Se entiende como red convergente a la red que es capaz de brindar servicios de transmisión de datos, voz y video sobre la misma red corporativa. Luego de la entrevista preliminar con personal de la empresa, se llegó a la conclusión que la transmisión de video para videoconferencias u otros usos no será considerada.

Este concepto pasó de ser una idea del futuro a ser una realidad en empresas de todos los tamaños y sectores comerciales. Los responsables de TI tienen la opción de centralizar el control y la gestión de diferentes soluciones en una misma plataforma, con el consiguiente ahorro en tiempo y recursos, mejorando así la efectividad, la eficiencia y la productividad de sus respectivas empresas.

2.3.1.1 Módulo de Campus

En el diseño del módulo de Campus se debería incluir los dispositivos listados en la Tabla 23, adicionalmente habrá que cumplir con los requerimientos del punto 1.4 del capítulo 1, por lo que es necesario incorporar dispositivos para brindar las siguientes soluciones:

- Servicio de Voz sobre IP
- Protección en equipos finales y servidores (antivirus)
- Respaldo de información en puntos finales.

El servicio de Voz sobre IP incluye un servidor que preste dicha funcionalidad, teléfonos IP, además de la posibilidad de agregar nuevos dispositivos como switches que permitan transmitir la voz a través de la red. De tal manera la Tabla 24 incorpora dispositivos a la Tabla 23 cumpliendo así con el análisis de requerimientos.

Equipo de comunicación	Cantidad requerida	Tiene	No tiene
Switches Capa 2	2		X
Servidor dedicado Voz sobre IP	1		X
Servidor Administración de Antivirus.	1		X

Equipo de comunicación	Cantidad requerida	Tiene	No tiene
Servidor Administración de respaldos de información.	1		X
Servidor de impresión	1	X	
Servidor de archivos	1	X	
Servidor AD (DNS – DHCP)	1	X	
Servidor Proxy	1	X	
Access Point	1		X
Teléfonos IP	50		X
Computadores	50	X	
Impresoras	4	X	

Tabla 25. Equipos necesarios en el módulo Campo
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

2.3.1.1.1 Plan de direccionamiento IP y VLANS

Al analizar los requerimientos, la estructura física y organizacional, se determinó que existen tres grupos definidos en la red local de la empresa KUEHNE+NAGEL división PERECIBLES, por lo que es necesario realizar una división de esta estructura lógica, logrando así la segmentación de tráfico, seguridad de la red, calidad de servicio y facilidad de administración.

Una VLAN es un método o una manera de crear redes lógicas independientes entre sí dentro de la misma red física, viéndose esto reflejado en la reducción de dominio de broadcast y facilitando la administración de las mismas.

Para el nuevo direccionamiento IP se utilizarán subredes creadas utilizando VLSM (Variable Length Subnet Mask). Considerando que el servicio de telefonía IP no estuvo considerado en el levantamiento inicial de información, en la Tabla 26 se detalla las VLANs a ser creadas.

VLAN	Identificación
Servidores	10
Telefonía IP	20
Usuarios	30
Invitados	40

Tabla 26. Nombre y número de identificación de VLANS
Elaborado por el autor

En la VLAN Servidores se encontrarán todos los servidores físicos además del host VMWare que contiene los servidores virtuales los cuales deben tener asignada una dirección IP fija independiente del host VMware.

La VLAN Telefónica tiene el objetivo de segmentar todo el tráfico de voz con respecto al tráfico generado por los usuarios y servidores.

La VLAN Usuarios es el segmento de red utilizado por los usuarios regulares de la empresa KUEHNE+NAGEL división PERECIBLES. Adicionalmente la empresa dispone de 4 impresoras IP las cuales serán incluidas dentro de esta VLAN.

La VLAN Invitados estará destinada para usuarios externos a la empresa y para usuarios que necesiten hacer uso de dispositivos Wireless como teléfonos inteligentes y tabletas entre otros.

Dado que la cantidad de usuarios de la red es de 50 y la proyección estimada de crecimiento será hasta máximo 60 usuarios, así mismo el número de teléfonos IP, la VLAN de Telefonía IP y la VLAN de usuarios dispondrá de 62 direcciones IP utilizables como se muestra en la Tabla 27.

Servicio/ Función	Subred / Mascara de subred	Número de direcciones IP disponibles
SERVIDORES	10.5.130.0/28	14
DATOS	10.5.130.16/26	62
VOZ	10.5.130.80/26	62
INVITADOS	10.5.130.144/26	62

Tabla 27. Nuevo Direccionamiento IP - KUEHNE+NAGEL división PERECIBLES
Elaborado por el autor

De esta manera, teniendo en cuenta el número de usuarios de la red, se ha propuesto un direccionamiento más lógico, permitiendo el ingreso de nuevos usuarios a la red.

Además, para el control de usuarios y administración de equipos, las estaciones de trabajo contarán con direccionamiento estático y no dinámico como hasta ahora. Esto incluye asignar dirección IP a los teléfonos IP. Las primeras direcciones IP serán utilizadas para los servidores físicos o virtuales. Esta determinación se realizó tomando en cuenta que la cantidad de usuarios no es demasiado grande, por lo que es posible mantener un inventario de direcciones IP.

2.3.1.2 Módulo de Internet Corporativo

En la Tabla 28, se muestran tanto los dispositivos existentes como los dispositivos que se necesitarán incorporar según los lineamientos de SAFE para el módulo de Internet.

Equipo de comunicación	Cantidad requerida	Tiene	No tiene
Firewall	1		X
Router	1	X	
Switch capa 3	1	X	
IPS/IDS	1		X

Tabla 28. Componentes requeridos en el módulo Internet Corporativo.
Fuente: Empresa Kuehne+Nagel UIO - TI
Elaborado por el autor

La figura 15 muestra el diagrama de red propuesta para la empresa KUEHNE+NAGEL división PERECIBLES, incluyendo los dispositivos existentes como los requeridos tanto en el módulo de campus como en el módulo de Internet.

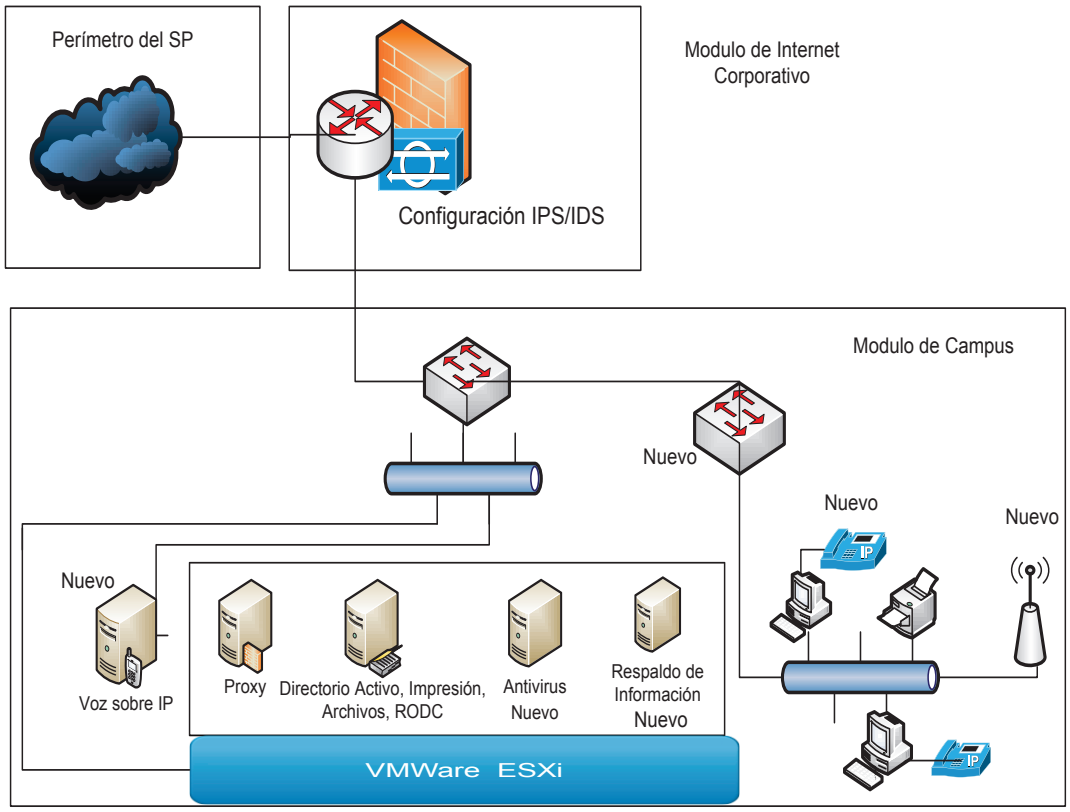


Figura 15. Diseño de red de KUEHNE+NAGEL división PERECIBLES.
Fuente: Metodología SAFE CISCO
Elaborado por el autor

2.3.2 DISEÑO DE SEGURIDADES DE LA RED

Con base en el punto 1.4.2.11, una vez seleccionados los controles es necesario plantear políticas o procedimientos que lleven al cumplimiento de los objetivos de control.

Los objetivos de control seleccionados son:

- Seguridad de los equipos
- Protección contra código malicioso
- Responsabilidad sobre los activos
- Requisitos de negocio para el control de accesos
- Responsabilidades del usuario
- Gestión de acceso de usuario
- Áreas seguras
- Control del acceso a sistemas y aplicaciones
- Copias de seguridad

2.3.2.1 Diseño de políticas de seguridad

2.3.2.1.1 Política de Seguridad de los equipos.

Objetivo

Evitar la pérdida, daño, robo o el comprometimiento de los activos y la interrupción de las operaciones de la organización

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de Implementación**: **(instalaciones de suministro)**
  - Adquisición, configuración y mantenimiento de sistema de alimentación alterno para la empresa con el objetivo de proteger equipos, servidores, dispositivos de red.
- ✓ **Guía de implementación (Seguridad del cableado)**
  - Cableado de energía eléctrica y telecomunicaciones debería estar ser instalado con todas las medidas de protección.
  - Planificación de la renovación del cableado estructurado existente.

- ✓ **Guía de Implementación (Mantenimiento de equipos)**
  - Generación de un plan de mantenimiento preventivo de equipos calendarizado, de acuerdo a las recomendaciones realizados por el fabricante.

Documento(s) de referencia

ISO/IEC 27001:2013

Objetivos de control: Seguridad de los equipos (12.2)

Control(es): Instalaciones de suministro (11.2.2)
Seguridad del cableado (11.2.3)
Mantenimiento de los equipos (11.2.4)

Desarrollo de la política.

Seguridad del cableado.

- ✓ El cableado estructurado dentro de la empresa deberá ser certificado de categoría 6e

- ✓ El Departamento de Sistema deberá llevar documentación organizada y actualizada de puntos de la red, puertos correspondientes a los puntos de red tanto en el Patchpanel de voz como en el de datos.
- ✓ Los usuarios deberán velar por el mantenimiento del cableado estructurado y demás componentes alrededor de su estación de trabajo.
- ✓ Ejecutar mantenimiento preventivo cada 6 meses a cada equipo, servidor o dispositivo de red. Documentar el procedimiento (cumplimiento, hora y fecha).

Mantenimiento de los equipos

- ✓ Se deberá ejecutar mantenimiento preventivo de acuerdo al plan de mantenimiento preventivo a cada equipo, servidor o dispositivo de red.
- ✓ Documentar o llevar una bitácora actualizada acerca del mantenimiento preventivo y/o correctivo de los equipos (cumplimiento, hora y fecha).
- ✓ Realizar un inventario de hardware de la empresa, incluir vida útil del dispositivo, garantías validas, garantía caducada.
- ✓ La información de los equipos que se dieran de baja por daño físico o fin de vida útil deberá ser borrada utilizando métodos de borrado seguro, previo la obtención de una copia de seguridad en caso de requerirlo.

Instalaciones de suministro

- ✓ Generación de un plan de mantenimiento preventivo de equipos calendarizado, de acuerdo a las recomendaciones realizados por el fabricante.
- ✓ Mantener actualizado el soporte técnico externo de los servicios de apoyo contrato.
- ✓ Redundancia en la conectividad de red, dispositivos de red locales, enlaces a Internet.
- ✓ Se deberá ejecutar mantenimiento preventivo de acuerdo al plan de mantenimiento preventivo de servicios de apoyo

2.3.2.1.2 Política de protección contra código malicioso.

Objetivo:

Asegurar que la información y los medios de procesamiento de información estén protegidos contra código malicioso o malware.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES y a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de Implementación**:
  - Instalación, configuración y mantenimiento de una solución licenciada de antivirus en equipos y servidores de la empresa.
  - Establecimiento de una política formal que prohíba el uso de software no autorizado.
  - Comunicación detallada, apropiada y oportuna de riesgos asociados con software no autorizado, sitios web sospechosos así como de archivos obtenidos de sitios red de externas o cualquier otro medio.
  - Definición de procedimientos y responsabilidades para lidiar con protección contra software malicioso en los sistemas.

Documento(s) de referencia:

ISO/IEC 27001:2013

Objetivos de control: protección contra código malicioso (12.2)

Control: Controles contra código malicioso (12.2.1)

Desarrollo de la política.

- ✓ Cada dispositivo de la empresa, entendiéndose por dispositivo a equipo de usuario final o servidor, deberá tener instalado y habilitado software antivirus autorizado por Departamento de Sistemas de KUEHNE+NAGEL división PERECIBLES para verificar la presencia de virus.
- ✓ Cualquier usuario que intuya la existencia de un virus debe realizar una revisión de sus archivos con el antivirus.
- ✓ Los programas para verificar la presencia de virus, autorizados por el Departamento de Sistemas de KUEHNE+NAGEL división PERECIBLES, deben estar activos constantemente en todos los servidores de redes de área local y de los computadores personales conectados a la red.
- ✓ Todos los archivos descargados de fuentes ajenas a la Empresa, a través de Internet o cualquier otra red pública, deben ser explorados con software antivirus, antes de que el software sea utilizado o los archivos examinados por otros programas.
- ✓ El departamento de Sistemas deberá preparar un taller de inducción a la solución antivirus con el fin de preparar al usuario en caso de incidentes relacionados con software malicioso.

2.3.2.1.3 Política de requisitos del negocio para el control de acceso.

Objetivo

Limitar el acceso a la información y a los medios de procesamiento de información.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de implementación**:
  - Comunicación detallada, apropiada y oportuna de políticas de control de acceso, derechos de acceso y restricciones de uso de la información o medios de procesamiento de la información indicando los riesgos de seguridad asociados con este manejo.
  - Los controles de acceso son tanto lógicos como físicos y deberían ser considerados juntos.
  - Comunicación acerca de obligaciones contractuales y legales acerca de las limitaciones de acceso a información o servicios.
  - Establecimiento de reglas basada en la premisa "Todo es generalmente prohibido a menos de que esté expresamente permitido".

Documento(s) de referencia

ISO/IEC 27002:2013

Objetivos de control: Requisitos de negocios para el control de acceso (9.1)

Control(es): Política de control de acceso (9.1.1)

Control de acceso a las redes y servicios adicionales (9.1.2)

Desarrollo de la política

- ✓ Los usuarios no deben tener acceso a información perteneciente a otro usuario sin previo consentimiento del jefe de departamento.
- ✓ La contraseña para acceso al o los medios de procesamiento de información deberá ser robusta (mínimo 6 caracteres, números y letras).

2.3.2.1.4 Política de responsabilidades sobre los activos

Objetivo

Identificar activos de la organización y definir las responsabilidades de protección adecuadas.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de implementación**:
  - Comunicación oportuna de buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

Documento(s) de referencia

ISOC/IEC 27002:2013

Objetivos de control: Responsabilidad sobre los activos (8.1)

Control: Uso aceptable de los activos (8.1.3)

Desarrollo de la política

- ✓ La contraseña de cada usuario es personal e intransferible, no puede ser divulgada ni entregada a ningún otro usuario sin previo consentimiento del jefe de departamento, si se lo requiere.
- ✓ No usar la misma información de autenticación para propósitos del negocio o fuera de él.

- ✓ Socialización de responsabilidad sobre el uso de activos (equipos e información).
- ✓ El computador y los sistemas de comunicaciones de la Empresa deben usarse únicamente para propósitos de negocio, salvo que se haya obtenido un permiso especial del jefe de departamento o TI.
- ✓ El uso personal del computador y de los sistemas de comunicaciones debe ser consecuente con las normas convencionales de conducta cortés y ética.
- ✓ El uso de la información de la Empresa para algún propósito que haya sido expresamente establecido por la gerencia debe ser aprobado por escrito por el dueño de datos designado.
- ✓ Solo el Departamento de Sistemas está autorizado a la instalación y/o desinstalación de cualquier software o aplicativo. Dicho proceso deberá ser documentado, indicando hora, motivo y usuario dueño del activo.
- ✓ Cualquier cambio de dispositivos de hardware se lo deberá comunicar por escrito o vía correo electrónico al Departamento de Sistemas.
- ✓ El jefe de departamento debe autorizar el uso que se da a los servicios de procesamiento de información y los controles que se deben aplicar para prevenir el uso indebido de los servicios.
- ✓ Todo usuario debe estar correctamente capacitado tanto física, técnica como emocionalmente para hacer uso de los sistemas de información como aplicaciones Web que involucran información de la empresa.
- ✓ Se deberá programar talleres de inducción sobre el uso de la información a través de los distintos medios de procesamiento.

2.3.2.1.5 Política de gestión de acceso al usuario.

Objetivo

Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de Implementación**:
  - Los derechos de acceso deberían ser revisados a intervalos regulares después de que el usuario sea objeto de ascenso, remoción o cualquier cambio en la organización.
  - Las autorizaciones para derechos de acceso elevado deberían ser revisadas con más frecuencia.
  - El departamento de Sistemas debe garantizar que los usuarios tengan los privilegios adecuados para la manipulación de información como privilegios de usuario estándar en cada equipo

Documento(s) de referencia

ISO/IEC 27002:2013

Objetivos de control: Gestión de acceso al usuario (9.2)

Control(es): Revisión de derechos de acceso de los usuarios (9.2.5)

Desarrollo de la política.

- ✓ Solo el Departamento de Sistemas puede ingresar local o remotamente a los servidores y otros dispositivos de red como switches o Router de la empresa.
- ✓ Se deberá documentar cualquier cambio dentro del Servidor Directorio Activo, es decir cambio o restablecimiento de usuario y/o contraseñas de acceso a la red.
- ✓ Se deberán documentar todos los cambios a nivel de configuración en cualquier dispositivo de red como Switches o Router de la empresa.

- ✓ Cualquier solicitud de cambio en los privilegios de acceso de un usuario deberá ser realizada vía correo electrónico.

2.3.2.1.6 Política de responsabilidades del usuario

Objetivo

Garantizar que los usuarios salvaguarden su información de autenticación.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de Implementación**:
  - o Comunicación oportuna de buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

Documento(s) de referencia

ISO/IEC 27002:2013

Objetivos de control: Responsabilidades del usuario (9.3)

Control(es): Uso de información confidencial para la autenticación (9.3.1)

Desarrollo de la política.

- ✓ La contraseña de cada usuario es personal e intransferible, no puede ser divulgada ni entregada a ningún otro usuario sin previo consentimiento del jefe de departamento, si se lo requiere.

- ✓ No usar la misma información de autenticación para propósitos del negocio o fuera de él.

2.3.2.1.7 Políticas de áreas seguras.

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los medios de procesamiento de información crítica o confidencial.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de implementación**:

  Utilización por parte de los usuarios de sistemas de seguridad como dispositivos biométricos, uso de tarjeta magnética, lector de huella digital o palma de la mano, para protección de áreas que contengan información y recursos para su procesamiento.

  Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Documento(s) de referencia

ISO/IEC 27002:2103

Dominio: Seguridad física y ambiental (11)

Objetivos de control: Áreas seguras (11.1)

Control(es): Perímetros de seguridad física (11.1.1)
Controles físicos de entrada (11.1.2)
Protección contra amenazas externas y ambientales (11.1.4)

Desarrollo de la política.

Controles físicos de entrada

- ✓ El acceso a cualquier área de trabajo que contenga información sensible estará restringido para personas no autorizadas.
- ✓ El acceso de visitantes o terceros a las oficinas de la Empresa, y otras áreas de trabajo que contengan información confidencial, debe ser controlado por guardias, recepcionista u otro personal.
- ✓ En caso de ingresar a un área restringida, el usuario deberá comunicar de este particular al jefe de departamento.

Protección contra amenazas externas y ambientales

- ✓ Rotular correctamente las indicaciones de salida de emergencia, áreas restringidas, ubicación de extintores, rutas de escapes en las instalaciones de la empresa con el fin de que los usuarios puedan elegir que acción tomar en caso de un evento inesperado.
- ✓ Revisar la carga de los extintores periódicamente para ser usados en caso de incendio.

2.3.2.1.8 Políticas del control del acceso a sistemas y aplicaciones

Objetivo

Prevenir el acceso no autorizado a los sistemas y aplicaciones**.**

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

- ✓ **Guía de implementación.**
  - Aplicaciones o servicios para respaldos de información deberían ser implementados para asegurar que la información esencial podrá estar disponible si ocurriese un desastre.
  - Diseño de un plan de respaldos de información que incluya tipo de información a respaldar, periodos de retención, destino del respaldo, tipo de respaldo, frecuencia del respaldo.
  - Diseño de un plan de simulación de recuperación ante desastres.

Documento(s) de referencia

ISO/IEC 27002:2013

Objetivos de control: Control de acceso a sistemas y aplicaciones

Controles: Restricción del acceso a la información

Gestión de contraseñas de usuario.

Desarrollo de la política.

- ✓ El departamento de Sistemas deberá restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados.
- ✓ Ningún usuario podrá acceder a aplicaciones o información de uso restringido sin previo aviso al Jefe de departamento.
- ✓ El departamento de Sistemas deberá controlar los derechos de acceso de usuarios como lectura, escritura, borrado y ejecución.

Gestión de contraseñas del usuario

- ✓ El departamento de Sistemas deberá recomendar no usar la misma contraseña a los usuarios para iniciar sesión en las distintas aplicaciones o medios de procesamiento a los que esté autorizado.
- ✓ Permitir a los usuarios seleccionar y cambiar sus propias contraseñas a sistemas de procesamiento de información como equipos de usuarios.
- ✓ Crear un usuario Administrador o en su defecto un usuario con privilegios elevados en cada uno de los equipos de usuario final.

2.3.2.1.9 Políticas de copias de seguridad.

Objetivo

Proteger a la organización contra la perdida de datos o información sensible o no sensible.

Alcance

Este documento aplica a la empresa KUEHNE+NAGEL división PERECIBLES, a la información confidencial y no confidencial que se maneja dentro de los procesos para la entrega de servicios.

Usuarios y responsables

Los usuarios de este documento son empleados de la empresa KUEHNE+NAGEL división PERECIBLES.

El responsable es el departamento de TI, se plantea una guía de implementación.

Documento(s) de referencia

ISO/IEC 27002:2013

Objetivo de control: copias de seguridad (12.3)

Control(es): Copias de seguridad de la información (12.3.1)

Desarrollo de la política.

- ✓ El departamento de Sistemas deberá instalar, configurar y mantener de una solución para manejo de respaldos de información de equipos y servidores.
- ✓ El departamento de Sistemas deberá comunicar oportunamente el tipo y frecuencia de respaldos de información en los equipos de los usuarios.
- ✓ El departamento de Sistemas deberá generar respaldos completos e incrementales actualizados.
- ✓ La información de negocios indispensable y los respaldos de software deben ser almacenados en un sitio aislado de la intemperie, con controles de acceso y a una distancia prudencial de la sede donde fueron generados.
- ✓ Los archivos de audio y video no serán respaldados.
- ✓ Los archivos con extensión .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, serán respaldados siempre y cuando se encuentren en la ubicación “Mis Documentos” correspondientes a cada perfil de usuario.
- ✓ Si el usuario desea respaldar algún tipo de archivo en especial deberá comunicar por escrito o vía correo electrónico al Departamento de Sistemas para solventar este requerimiento.
- ✓ El departamento de Sistemas deberá comprobar regularmente el estado de los respaldos, tanto de servidores como de información del usuario final.

2.3.3 DIMENSIONAMIENTO DE LA RED PASIVA

El diseño de la red pasiva radica en realizar el dimensionamiento de los elementos necesarios para conformar el sistema de cableado estructurado para la red LAN, cumpliendo con estándares internacionales.

2.3.3.1 Cableado estructurado

El cableado estructurado es un conjunto de cables y demás elementos como conectores, el cual permite la conexión entre los dispositivos de red como equipos finales, teléfonos IP, impresoras, servidores como los equipos de comunicación como switches y Router, independientemente del fabricante de los equipos o dispositivos.

El diseño del cableado estructurado incluye subsistemas como:

- Cableado Horizontal
- Área de trabajo
- Cuarto de equipos y telecomunicaciones
- Cableado Vertical.

2.3.3.1.1 Cableado Horizontal

Para el cálculo del cableado horizontal se utilizará el método aproximado, debido a que en las visitas realizadas se puedo obtener medidas cercanas a la realidad, utilizando además el diagrama del Anexo 1. Este método busca determinar los rollos de cable utilizando la distancia máxima, la distancia mínima y la cantidad de puntos a instalar.

$$d1 = \frac{dist.\max + dist.min}{2}$$

$$d1 = \frac{45 + 4}{2}$$

$$d1 = 24.5$$

Se calcula un 10% de holgura, así:

$$d2 = d1 * 1.1$$

$$d2 = 24.5 * 1.1$$

$$d2 = 26.95$$

Se calcula el número de corridas por caja, así:

$$d3 = \frac{305}{d2}$$

$$d3 = \frac{305}{26.95}$$

$$d3 = 11.31$$

Finalmente, con el valor d3 se puede calcular el número de rollos.

$$número\ de\ rollos = \frac{\#\ de\ puntos\ de\ red}{d3\ aproximado}$$

$$número\ de\ rollos = \frac{55}{11}$$

$$número\ de\ rollos = 5.0$$

La topología del cableado estructurado seguirá la norma TIA/EIA 568-C, es decir la topología será tipo estrella. Los beneficios de utilizar un correcto cableado estructurado con los estándares actuales son enormes, entre ellos:

- Disminuir la posibilidad de que el cableado sea parte de una posible amenaza a la estabilidad de la red,

- Incrementar la velocidad para la transmisión de los datos en comparación con un cableado más antiguo, por lo tanto, el funcionamiento y las prestaciones de la red será más eficiente.

2.3.3.1.2 Área de trabajo

El área de trabajo está constituido por: puntos de red, salida de telecomunicaciones y Patch Cords.

2.3.3.1.2.1 Puntos de red

La distribución de los puntos red y cantidad se determinó mediante las visitas realizadas y a la información proporcionada por el Departamento de Sistemas de KUEHNE+NAGEL división PERECIBLES, la Tabla 29 muestra la cantidad de puntos de red y voz requeridos.

Ubicación	Puntos de Datos	Puntos de Voz	Total
KUEHNE+NAGEL división PERECIBLES	55	50	105

Tabla 29. Puntos de red KUEHNE+NAGEL división PERECIBLES.
Elaborado por el autor

2.3.3.1.2.2 Salida de telecomunicaciones

Las salidas de telecomunicaciones básicamente están estructuradas por un cajetín, un face plate simple o doble y un Jack que en este caso será RJ-45. Dichas salidas estarán ubicadas cerca de cada puesto de trabajo permitiendo al usuario acceder a la red de voz y datos en su estación de trabajo. En la Tabla 30 se detalla la cantidad de face plate simples y face plate dobles.

Ubicación	FacePlate Simple	FacePlate Dobles	Total
KUEHNE+NAGEL división PERECIBLES	5	50	55

Tabla 30. Cantidad de Face Plates.
Elaborado por el autor

2.3.3.1.2.3 Patch Cord

Los cables de conexión que van desde los equipos de los usuarios, ya sean computadores o teléfonos IP, hasta la salida de telecomunicaciones son conocidos como Patch Cord. Para este proyecto, se utilizarán Patch Cords categoría 6 de cuatro pares y conectores RJ-45, igualmente categoría 6.

La longitud promedio del Patch Cord oscila entre los dos a tres metros debido a la movilidad que se pueda requerir, la cantidad de Patch Cords varía ya que es importante tener dentro del inventario una cantidad adecuada de Patch Cords, en este caso se considerarán setenta y cinco (75) Patch Cords como se ve en la Tabla 31.

	Cantidad de Patch cord
KUEHNE+NAGEL división PERECIBLES	75

Tabla 31. Cantidad de Patch Cord.
Elaborado por el autor

2.3.3.1.3 Cuarto de equipos y telecomunicaciones

El cuarto de equipos y el cuarto de telecomunicaciones, estructuralmente, varían ya que el cuarto de equipos es un lugar especializado en el alojamiento de

equipos como servidores o la central telefónica, el cuarto de telecomunicaciones alberga uno o varios switches para proveer servicios de voz y datos a una determinada dependencia o piso en el caso que se tratase de un edificio. Para este proyecto, al tratarse de una sola planta los dos cuartos se ubicarán dentro del espacio físico predeterminado.

En las visitas realizadas se constató que el rack de comunicaciones no se encuentra debidamente organizado por lo que es necesario incluir accesorios de cableado como:

- Regletas multitomas
- Organizadores horizontales
- Bandeja para fibra
- Patch pannels de 48 puertos

El rack dispone de 8U por lo que no es necesario realizar la compra de uno adicional.

2.3.3.1.4 Cableado Vertical

El cableado vertical para este proyecto no se lo considerará debido a que la empresa KUEHNE+NAGEL división PERECIBLES labora únicamente en una dependencia física, no es necesario interconectar el cuarto de telecomunicaciones o equipos con otros cuartos de las mismas funciones. Además, la corporación encargada de la construcción de Aeropuerto en Tababela, ha planificado e instalado todo el cableado vertical, por lo que tanto la empresa KUEHNE+NAGEL división PERECIBLES como las demás empresas que laboran en el nuevo Aeropuerto no se ocuparán de este aspecto, únicamente del cableado horizontal.

2.3.4 DIMENSIONAMIENTO DE LA RED ACTIVA

La selección de los dispositivos de red y equipos necesarios para el brindar los servicios que los usuarios requieren como el servicio de VoIP, protección de

puntos finales, respaldos de información para la empresa KUEHNE+NAGEL división PERECIBLES constituyen la elección de los elementos constitutivos de la red activa.

De acuerdo a la Tabla 25 y 28, se requieren de los siguientes dispositivos de red y servidores, detallados en la Tabla 32, para cumplir tanto con el análisis de requerimientos como con el diseño de seguridad que plantea SAFE Cisco.

Modulo	Equipos	Cantidad
Campus	Switch capa 2	2
	Servidor de Antivirus	1
	Servidor de Respaldos de información	1
	Servidor dedicado Voz sobre IP y elementos adicionales (Gateway de voz)	1
	Teléfonos IP	50
	Access Point	1
Internet	Firewall IDS/IPS	1

Tabla 32. Resumen de elementos requeridos.
Elaborado por el autor

La Tabla 33 contiene los sistemas requeridos como parte del cumplimiento de implantación de controles específicos de la Tabla 16, según la norma ISO/IEC 27002:2013

	Sistemas
Seguridad Física	UPS - Sistema de suministro alterno de energía eléctrica.
	Sistema Contra Incendios
	Sistema de control de acceso

Tabla 33. Sistemas requeridos para brindar seguridad física.
Elaborado por el autor

Los elementos de la red y los sistemas para el aseguramiento físico de las instalaciones listados en las Tablas 32 y 33, respectivamente, deberían cumplir con ciertas características mínimas, las mismas que se describen a continuación.

2.3.4.1 Dispositivos de red

Con el objetivo de garantizar que el servicio telefónico no se vea interrumpido, además de disminuir el número de cables que rodeen un puesto de trabajo, se debe confirmar que los Teléfonos IP funcionarán con la tecnología PoE de las siglas PowerOver Ethernet. Esta tecnología básicamente establece que los teléfonos recibirán la alimentación eléctrica necesaria mediante el cable UTP.

Para el caso de PoE, se necesita que los switches de acceso actúen como fuente de alimentación, son llamados PSE[12] y los teléfonos serán los dispositivos que serán alimentados eléctricamente o también llamados PD.[13] Además de PoE, los dispositivos de red requieren de las siguientes características.

2.3.4.1.1 Características técnicas de Switch de capa 2

[12] Power Source Equiment
[13] Powered Equiment

- 48 Puertos de 10/100/1000 Mbps
- 2 puertos 10/100/1000 Mbps
- Soporte de VoIP
- PoE (Power over Ethernet)
- QoS (Calidad de servicio)
- Velocidad de conmutación (Throughput) : 6 Mbps
- Capacidad de conmutación (Backplane): 11.6 Gbps
- Administrable
- Capa OSI 2
- Estándares IEEE
    - 802.3x
    - 802.3ad
    - 802.1p
    - 802.1q (Soporte VLANs)
    - 802.1x
    - 802.1u
- Filtrado basado en MAC.
- Bajo consumo de energía.

2.3.4.1.2 Características técnicas del Access Point

- Cumplimiento de la norma IEEE 802.11 a/b/g/n
- Compatibilidad IEEE 802.3af (PoE).
- Cumplimiento de estándares de seguridad WPA, WPA2, 802.11i y 802.1x
- Mecanismo de autenticación EAP: TLS, TTLS, PEAP
- Frecuencia de funcionamiento de 2.4 GHz y 5 GHz
- Control de acceso a través de MAC.
- Protocolos de gestión remota SNMP, telnet, HTTP.

2.3.4.1.3 Firewall con IPS/IDS

Para cumplir con las guías de diseño que plantea SAFE Cisco para el módulo de Internet Corporativo, es necesario incluir en el diseño un equipo que cumpla con las funciones de IDS/IPS, sistema de detección de intrusos/sistema de prevención de intrusos por sus siglas en ingles respectivamente.

Las tecnologías de IPS/IDS presentan cambios e innovaciones notables que mejoran su capacidad de detección de intrusiones. Muchos productos IPS/IDS basados en red y host han añadido el uso de servicios de reputación. Estos servicios llevan años en uso por otras herramientas de control de seguridad. Los servicios de reputación reúnen información sobre lo bueno o malos que son ciertos dominios, direcciones IP, protocolos, ubicaciones físicas y otros aspectos de la actividad de la red. Los sistemas IPS/IDS usan esta información para ver si la actividad en estudio puede ser buena o no.

El Router CISCO891 es un Router de servicios integrados, que combinan el acceso a Internet, seguridad, voz, el apoyo de Metro Ethernet, y servicios avanzados de IP en un solo dispositivo; éste incluye las siguientes características:

- Firewall de inspección de estado de paquetes (SPI).
- Sistema de prevención de intrusiones (IPS)
- Enrutamiento dinámico y calidad de servicio avanzada (QoS).
- 20 túneles VPN IPSec para acceso remoto.

Por lo tanto no es necesario adquirir un nuevo equipo, sino más bien, realizar la configuración necesaria para implementar el sistema de prevención de intrusos.

2.3.4.1.4 Soluciones para Voz sobre IP

Para el diseño y dimensionamiento de la red de telefonía IP para la empresa KUEHNE+NAGEL división PERECIBLES se considerará una solución que preste este servicio mediante el uso de software libre.

2.3.4.1.4.1 Central Telefónica IP

La solución para brindar el servicio de telefonía IP que se elija deberá cumplir con ciertas características que se detallan a continuación.

- Capacidad para brindar el servicio para al menos 50 usuarios de la red KUEHNE+NAGEL división PERECIBLES
- Permitir la conexión con PSTN (red telefónica pública).
- Protocolos de señalización
- Control de llamadas
- Administración Web, entre otras.

En el mercado existen varias opciones para centrales telefónicas, tanto propietarias como basadas en Software Libre, para este proyecto se optará por la segunda opción. En este contexto, dentro del mercado existen varias soluciones de telefonía IP basados en Asterisk como Elastix, SwitchVox, Trixbox, entre otras; cada una de estas con sus características particulares. En este proyecto se utilizará la Central Telefónica IP Elastix.

Elastix puede funcionar correctamente bajo arquitectura x86 como en x64, además puede ser virtualizado por lo que es una opción válida para la implementación en la empresa, considerando que el Sistema Asterisk hace las funciones de central IP-PBX y Gateway de voz

En la Tabla 34 se describen los requerimientos mínimos de hardware para los distintos entornos en los que se desee implementar el sistema de telefonía VoIP.

Entornos	Número de extensiones	Requerimientos mínimos
Pequeños	Hasta 15	X86 de 400 MHz – 512 RAM
Medianos	Entre 15 y 50	X86 de 1 GHz – 1 RAM

Grandes	Entre 50 y 100	X86 de 1.5 GHz – 3 RAM
Muy Grandes	Más de 100	Arquitecturas distribuidas

Tabla 34. Requerimientos de hardware para instalación de Elastix.
Elaborado por el autor

La solución de telefonía IP Elastix será instalada en una máquina virtual dentro del host detallado en la Tabla 4. y tendrá las siguientes características.

Sistema Operativo:	Centos 6.0
Número de Procesadores:	4
Memoria RAM:	6 GB
Espacio en disco:	80 GB
Interfaz de red:	Switch Virtual dedicado

2.3.4.1.4.2 Teléfonos IP

Los teléfonos IP para los diferentes usuarios de la empresa KUEHNE+NAGEL división PERECIBLES deberán tener las siguientes características:

- Soporte PoE (IEEE 802.3af)
- Dos puertos 10/100/1000 Mbps
- Soporte para codecs G.729 y G.711
- Soporte IEEE 802.1 p e IEEE 802.1Q
- Soporte Protocolo SIP y estándar H.323
- Identificación de llamadas
- Transferencia de llamadas
- Llamada en espera
- Tageo de VLANs

2.3.4.1.5 Características mínimas de Servidor Antivirus

- Sistema Operativo: Windows Server 2008 R2
- Memoria: 4GB
- Procesador: Dual Core
- Espacio en disco: 20 Gb
- Interfaz de red: 100/1000 Mbps

2.3.4.1.6 Características mínimas Servidor Respaldo de Información.

- Sistema Operativo: Windows Server 2008 R2
- Memoria: 4GB
- Procesador: Dual Core
- Espacio en disco: 20 GB
- Interfaz de red: 100/1000 Mbps
- Espacio de almacenamiento.: 500 GB disponibles

Para el cálculo del espacio requerido para almacenar la información se debe considerar lo siguiente.

- Cantidad de información a respaldar. Esta información debería ser obtenida realizando un promedio de información de cada usuario.
- Cantidad de usuarios.
- Versionamiento de archivos.

Por lo tanto, la Tabla 35 indica el espacio requerido para el almacenamiento de información de los usuarios.

Cantidad de usuarios	Cantidad de información (GB)	Versionamiento (unidad)	Total (GB)
50	5	2	500

Tabla 35. Espacio en disco requerido para respaldo de información.
Elaborado por el autor

Ambos servidores pueden ser Virtualizados, por lo que podrán ser incluidos dentro del host detallado en la Tabla 4.

2.3.4.1.7 Sistema de suministro alterno de energía eléctrica.

Características Generales del UPS

- Potencia: 6KVA
- Tecnología: En línea de doble conversión
- Frecuencia: 50/60 Hz
- Tiempo de respuesta: menor a 4 ms
- Tiempo de recarga de batería: menor a 5 horas.
- Duración promedio de reserva con carga total o completa: 9 minutos
- Duración promedio de reserva con carga media: 23 minutos

2.3.4.1.8 Sistema Contra Incendios

La empresa KUEHNE+NAGEL división PERECIBLES dispone de 2 extintores de dióxido de carbono, pero es recomendable la instalación de un sistema contra incendios, el cual está conformado por un sistema de detección y un sistema de extinción.

El sistema de detección deberá incluir:

- Al menos 2 detectores de humo.
- Led o luces indicadores de estado.

El sistema de extinción de incendios tendrá las siguientes características:

- Extinción de fuegos clase: A, B, C.
- Agente limpio, es decir un agente que pueda ser aplicado para extinción de fuegos tipo A,B o C sobre cualquier activo de gran valor como servidores, equipos de red entre otros.

- Amplia cobertura de extinción
- No tóxico para el ambiente ni para personas.

2.3.4.1.9 Sistema de control de acceso

Para el control de acceso al DataCenter se recomienda un sistema biométrico de control de acceso basado en la lectura de la huella digital, de esta manera se garantiza que acceso estará debidamente restringido.

Este tipo de sistema biométrico utiliza una cerradura electromagnética, además necesita de una dirección IP para ser administrado por un equipo adicional.

3. CAPITULO 3

PROPUESTA TÉCNICA-ECONÓMICA

3.1 INTRODUCCIÓN

En el presente capítulo se hace un análisis referencial de los costos de implementación del proyecto, incluyendo los equipos activos y pasivos, además de las soluciones enfocadas en seguridad de la información, con el objetivo de asegurar la disponibilidad, integridad y confidencialidad. La estimación del presupuesto para el proyecto fue realizado a partir de consultas realizadas a empresas proveedoras localizadas en la ciudad de Quito.

Más adelante, se describe el análisis de beneficio-costo realizado desde un enfoque técnico económico, considerando siempre la idea de que las soluciones o equipos de comunicación más caros no son, necesariamente, los mejores y viceversa.

A fin de establecer comparaciones que orienten la toma de decisiones, se proponen varias alternativas que cumplen con los requerimientos de seguridad previamente establecidos, incluyendo detalles de cada equipo de comunicación y de cada solución de seguridad propuesta.

3.2 INGENIERÍA DE DETALLE

Una vez establecidos los requerimientos de equipos de comunicación tanto activos como pasivos, detallados en el capítulo 2, es necesario realizar el listado detallado de dichos equipos para conocer la inversión económica que demandará la adquisición, instalación y el mantenimiento de la red.

3.2.1 RED PASIVA

La obra civil de las instalaciones de la empresa partió desde cero y ha estado avanzando a un ritmo relativamente lento por causas que no se analizarán en este proyecto, luego gracias al Departamento de Sistemas de la empresa, se realizó un diagrama que explica la posible distribución de los puestos de trabajo de la empresa, lo que determinará la cantidad de material necesario. Ver Anexo 1.

Con base en el punto 2.3.3.1.2, en la Tabla 36 se muestra el listado de los elementos necesarios para la implementación del sistema de cablea estructurado asi como de cantidad, el valor unitario y el valor total.

Elementos pasivos	Cantidad	Valor Unitario (USD)	Valor total (USD)
Cable UTP CAT 6A	5	197	985
Face Plate Simples	50	2,25	112,5
Face Plate Dobles	5	2,25	11,25
Regletas multitomas	2	63,25	126,5
Patch Cords	75	12,99	974,25
Jack RJ45 CAT 6A	55	11,89	653,95
Regletas multitomas	2	62	124
Bandeja de fibra	1	85	85
Organizadores horizontales	2	17	34
Organizadores Verticales	2	46	92
Patch panel de 48 puertos	2	220	440
Total			3638,45

Tabla 36. Costo del Sistema de Cableado Estructurado
Elaborado por el autor

Además de los elementos que conforman el sistema de cableado estructurado, en la Tabla 37 constan los valores por la instalación y certificación de los puntos de red.

Descripción	Cantidad de puntos	Valor Unitario (USD)	Valor total (USD)
Instalación de puntos de red	55	38	2090
Certificación categorización CAT 6	55	6	330
Total			2420

Tabla 37. Costo categorización e instalación.
Elaborado por el autor

3.2.2 RED ACTIVA

Como se puede observar en la Tabla 32, existen equipos de comunicación que necesitan ser adquiridos para completar el diseño de la red planteada, principalmente para brindar el servicio de Voz sobre IP.

3.2.2.1 Switch de acceso

La Tabla 38 muestra la comparación de características de switches de acceso de distintos fabricantes pero similares características.

Características requeridas	Switch de acceso	Switch de acceso
Marca	Hewlett Packard	Cisco
Modelo	2620	3560 V2
Cantidad de puertos	48x10/100 2X10/100/1000	48x10/100 2X10/100/1000
Soporte VoIP	SI	SI
Velocidad de conmutación (Throughput) :	6 Mbps	13.3 Mbps
Capacidad de conmutación (Backplane):	11.6 Gbps	16 Gbps
PoE	SI	SI
QoS	SI	SI

Administrable	SI	
Capa OSI 2	SI	SI
ACL	SI	SI
Estándares IEEE 802.3x, 802.3ad, 802.1p, 802.1q (Soporte VLANs), 802.1x, 802.1u	SI	SI
Filtrado Basado en puertos y MAC	Únicamente en puertos	SI
Consumo de energía gestionable	NO	SI

Tabla 38. Tabla Comparativa – Switch de capa 2
Elaborado por el autor

Los switches HP 2620 y el Cisco 2960 pertenecen a fabricantes mundialmente conocidos, la diferencia entre estos dos modelos es que los pertenecientes a la marca Cisco poseen mayor capacidad de enrutamiento/conmutación, cumplen y exceden las características mínimas descritas en el punto 2.3.4.1.1, Además los dispositivos del fabricante Cisco incorpora la tecnología EnergyWise, la cual permita gestionar de manera proactiva el consumo de energía de los dispositivos de red.

En la Tabla 39 se detalla el costo del Switch Cisco proporcionado por dos empresas de la ciudad de Quito.

Cantidad	Descripción	Modelo	Costo Intcomex (USD)	Costo Enlace Digital (USD)
1	Cisco Switch 48p PoE	WS-C2960S-48TD-L	1430,51	1378,74
IVA			171,66	165,78
Total			1602,17	1544,88

Tabla 39. Costo de switches de capa 2.
Elaborado por el autor

3.2.2.2 Access Point

Este dispositivo agregado adecuadamente a la red corporativa, nos permitirá brindar principalmente el servicio de acceso a internet wireless tanto para usuarios de la organización como para visitantes, en la Tabla 40 se realiza una comparación entre Access Point de distinto fabricante, en este caso Cisco y Ubiquiti.

Características requeridas	Access Point	Access Point
Marca	Ubiquiti	Cisco
Modelo	UAP	WAP4400N
IEEE 802.11 a/b/g/n	SI	SI
PoE	SI	SI
Cumplimiento de estándares de seguridad WPA, WPA2, 802.11i y 802.1x	SI	SI
Control de acceso a través de MAC.	SI	SI
Protocolos de gestión remota SNMP, telnet, HTTP	SI	SI

Tabla 40. Tabla Comparativa – Access Point
Elaborado por el autor

En el mercado existen muy buenas referencias acerca de la marca “Ubiquiti” para Access Points, esta marca combina rendimiento, escalabilidad ilimitada además de un precio razonable. En la Tabla 41 se encuentra el costo del Access Point de marca Ubiquiti.

Cantidad	Descripcion	Costo Intcomex	Costo Enlace Digital
1	Ubiquiti UAP UniFi Wireless N 2.4GHz Access Point	121,50	119,78
IVA		14,58	14,37
TOTAL		136,08	134,15

Tabla 41. Costo AP Ubiquiti.
Elaborado por el autor

3.2.2.3 Firewall IPS/IDS

El dispositivo de red CISCO891, descrito en el punto 2.3.4.1.6, tiene incorporado características técnicas de IDS/IPS las cuales no han sido debidamente configuradas por lo que es necesario que este trabajo sea realizado por un especialista, el cual realizará el trabajo de configuración y pruebas de funcionamiento, el costo de dicho trabajo se encuentra en la Tabla 42.

Descripción	Cantidad (horas)	Costo hora (USD)	Costo total (USD)
Configuración IPS/IDS y pruebas. Router Cisco 891	2	110	220

Tabla 42. Costo hora/hombre para configuración Firewall IDS/IPS.
Elaborado por el autor

3.2.3 SOLUCIONES VOIP

Como se remarcó en el punto 2.3.4.1.4 se optará por una solución de telefonía IP basada en software libre, la razón principal, además de las excelentes prestaciones y los mínimos recursos de hardware requerido, es el costo de instalación y mantenimiento, por lo tanto se ha seleccionado una solución de telefonía IP que utiliza equipos dedicados basados en el sistema Asterisk.

En la Tabla 43 se detalla el costo de la implementación de la solución de Voz sobre IP para la empresa, incluyendo capacitación respectiva.

Descripción	Cantidad (HORAS)	Costo Unitario (USD)	Costo Total (USD)
Instalación, configuración y pruebas de Central Telefónica Asterisk.	8	120	960
Capacitación	4	120	480
Total			1440

Tabla 43. Costo Instalación y configuración Central Elastix.
Elaborado por el autor

Los teléfonos IP deben cumplir con características básicas que deben cumplir los teléfonos IP, dichas características están listadas en la Tabla 44.

Características	Teléfonos IP	Teléfonos IP
Marca	Fanvil	Cisco
Modelo	C62	7965G
PoE	SI	SI
Taggeo de vlan	SI	SI
Soporte SIP	SI	SI
QoS	SI	SI
Soporte para codecs G.729 y G.711	SI	SI

Tabla 44. Tabla comparativa – Teléfonos IP.
Elaborado por el autor

En la Tabla 45, se detalla el precio total de los teléfonos IP de las marcas Fanvil y Cisco.

Cantidad	Fanvil	Grandstream
Costo Unitario (USD)	130	140,45
Cantidad	50	50
Total (USD)	6500	7022,5

Tabla 45. Costo de Teléfonos IP.
Elaborado por el autor

3.2.4 PROTECCIÓN DE PUNTOS FINALES

La intención de este proyecto es realizar un enfoque del diseño de la red corporativa global tomando en cuenta la mayor cantidad de aspectos de seguridad, esto incluye una solución centralizada contra virus, malware y spyware, sin dejar de lado el rendimiento del equipo del usuario ni el rendimiento de la red al momento de realizar actualizaciones de definiciones de virus o escaneos. Como se evidenció en las visitas, los equipos de escritorio no poseen antivirus licenciado lo que implica que la empresa tampoco posee soporte técnico para solucionar problemas de este aspecto.

Para la elección de proveedores, tanto de equipos como para productos de seguridad de TI, se utilizará uno de los principales puntos de referencia de selección de soluciones de software y hardware, el cuadrante de Gartner[14].

Gartner no respalda a ningún proveedor, producto ni servicio, ni aconseja a los usuarios de tecnología seleccionar solo a aquellos proveedores con las más altas calificaciones u otra designación, es una guía para las organizaciones, permitiéndoles tomar una decisión apoyada en estudios independientes, objetivos, basados en metodologías que consisten en prácticas de investigación.

[14] http://www.gartner.com/technology/research/methodologies/

El Cuadrante Mágico de Gartner está dividido en cuatro partes como se aprecia en la figura 16, en los cuales son ubicadas las compañías en función de su tipología y la de los productos y servicios que ofertan.

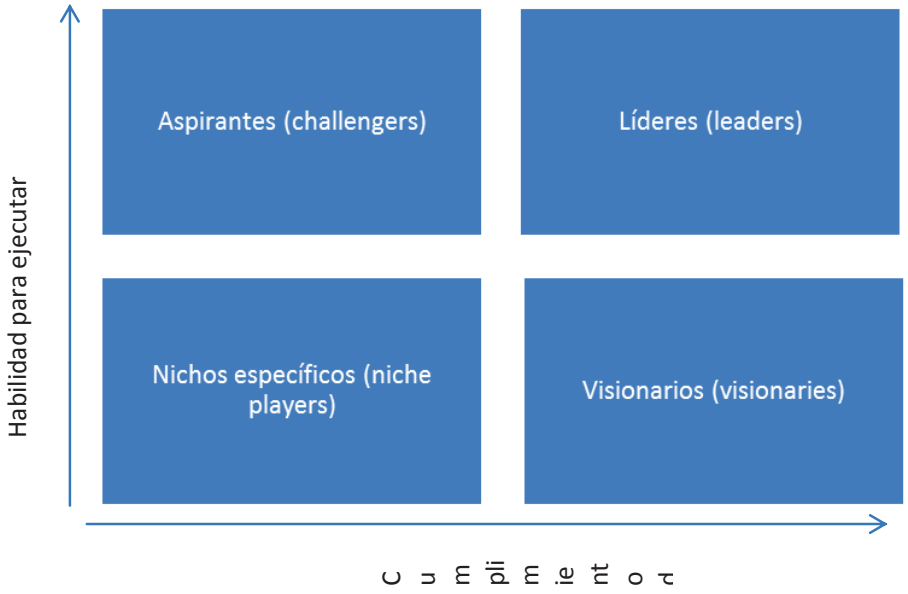


Figura 16. Cuadrante de Gartner
Fuente: Sitio Web: *www.**gartner**.com*
Elaborado por el autor

1) Líderes (leaders): aquellos que tienen la mayor puntuación resultante al combinar su habilidad para ejecutar (lo bien que un vendedor vende y ofrece soporte a sus productos y servicios a nivel global) y el alcance de visión, que se refiere a su potencial.

2) Aspirantes (challengers): caracterizados por ofrecer buenas funcionalidades y un número considerable de instalaciones del producto, pero sin la visión de los líderes.

3) Visionarios (visionaries): Visionarios son los que introducen nuevas tecnologías, servicios o modelos de negocio, pero su debilidad se encuentra en canales de distribución y en ventas. Ocasionalmente son absorbidos por empresas que se encuentran en los cuadrantes superiores.

4) Nichos específicos (niche players): enfocados a determinadas áreas de las tecnologías, pero sin disponer de una suite completa que les permita ser más competitivos

Figura 17. Cuadrante de Gartner para plataformas de protección de puntos finales[15]
Fuente: Reporte Gartner 2014

De la figura 17, se desprende que los productos que lideran el aspecto de protección de puntos finales son las soluciones de las marcas Symantec, McAfee y Kaspersky. La arquitectura de las soluciones descritas se basa en una consola centralizada, instalada en un servidor físico o virtual desde la cual se puede manejar políticas y reglas de funcionamiento de cada solución instalada en los equipos terminales.

Al momento de adquirir una solución para la protección de puntos finales se busca que la solución sea completa, es decir, que cumpla con:

[15] Fuente: Gartner Enero 2014

- Protección contra virus, malware y spyware.
- Firewall
- Protección para navegación.

En la Tabla 46 se realiza una comparación entre las soluciones de protección de puntos finales del mercado actualmente, con base en el cuadrante de Gartner

.

Características	Symantec	McAfee Antivirus Plus	Kaspersky
Protección contra virus, malware y spyware.	SI	SI	SI
Firewall	SI	SI	SI
Protección para navegación.	SI	SI	SI
IPS local	SI	NO	NO
Encriptación de disco	NO	NO	SI
Detección por reputación	SI	NO	SI
Uso de recursos (CPU)	Medio	Medio	Bajo
Licenciamiento por equipos	SI	SI	SI

Tabla 46. Soluciones de protección de puntos finales
Fuentes: Web-Site Symantec, McAfee, Kaspersky
Elaborado por el autor

Al igual que en el caso de las solución de respaldos de información, las empresas que brindan la solución de antivirus deberán instalar, configurar y mantener la solución con personal técnico certificado por el fabricante.

En la Tabla 47, se ha especificado el costo de las licencias y el costo de un paquete de horas de duración de un año para el manteniendo y soporte técnico de la solución.

Descripción	Symantec Endpoint Protection (USD)	Kaspersky Antivirus (USD)	McAfee (USD)
Costo licencia 60 usuarios	3600.00	2940.00	3120.00
Costo 10 Horas de soporte	500.00	450.00	450.00
Total	4100.00	3390.00	3570.00

Tabla 47. Costo Solución Antivirus.
Fuente: Departamento comercial empresas de seguridad
Elaborado por el autor

3.2.5 DISPONIBILIDAD DE LA INFORMACIÓN

Como se abordó en el punto 1.4.2, La disponibilidad de la información no solo se refiere a la protección de los documentos de cada usuario, sino también a almacenar en un repositorio seguro y confiable datos críticos de servidores de la empresa.

Como parte del cumplimiento de los controles seleccionados en el punto 1.4.2.11, es necesario proponer una solución para manejo de respaldo en forma eficaz y eficiente, asegurando así que la información de cada usuario o de los servidores permanezca disponible cuando este lo requiera.

La solución más efectiva sería la de utilizar una herramienta basada en el despliegue de agentes en cada servidor para obtener respaldos programados, este aspecto es importante puntualizarlo ya que una solución de respaldos debe ser totalmente transparente a los usuarios. Las tareas de respaldo suponen una carga extra al servidor ya que tiene procesar la de información proveniente de respaldos, por lo tanto lo más recomendable es que el servidor de respaldos sea un servidor físico pero considerando la cantidad de información que maneja la empresa a respaldar se propondrá un servidor virtual.

Usando como guía el Cuadrante de Gartner, la figura 18 muestra cómo los fabricantes CommVault y Symantec se encuentran a la vanguardia para el manejo de respaldos de información, por lo que en lo posterior se mencionará soluciones de seguridad ofertadas por estas empresas.

Figura 18. Cuadrante de Gartner para software de Respaldo y Recuperación[16]
Fuente: Reporte Gartner 2014

En este punto, es importante aclarar que plantear una solución de respaldo de información de puntos finales o servidores o el sistema de protección no supone una degradación de la red en su desempeño.

La herramienta de respaldo debe ser totalmente transparente a los usuarios, sin embargo, se debe establecer una comunicación adecuada entre TI y los usuarios sobre los cuáles la empresa implementará las políticas de respaldo, la Tabla 48

[16]Fuente: Gartner Junio 2014

muestra una comparación entre las característica de las soluciones para respaldo de información.

Características Principales	DLO Symantec	Simpana CommVault
Soporte para Windows	SI	SI
Deduplicación de datos	SI	SI
Respaldo en linea (en caliente	SI	SI
Uso de Agente para Windows y Mac	SI	SI
Priorización de uso de recursos	SI	NO
Compresión y encriptación.	Alta compresión	Media Compresión
Licenciamiento por equipo	No	SI

Tabla 48. Solución para respaldo y recuperación de información.
Fuente: Web-Site Symantec, CommVault
Elaborado por el autor

En la Tabla 49, se encuentra el costo de las licencias de uso de la solución de respaldos, además se añade el costo de un paquete de horas para la instalación, configuración y mantenimiento de la solución.

Descripción	Symantec Desktop and Laptop Option (USD)	CommVault Simpana (USD)
Costo licencia para 60 usuarios	3548	4080
Costo 10 Horas de soporte	500	500
Total	4048	4580

Tabla 49. Costo Solución respaldos de información
Fuente: Departamento comercial empresas de seguridad
Elaborado por el autor

3.2.6 SISTEMA DE SUMINISTRO ALTERNO DE ENERGÍA ELÉCTRICA.

A continuación en la Tabla 50 se muestra el costo de los módulos UPS, así como también el costo de la instalación del mismo, el cual servirá para abastecer de energía a equipos de comunicación y servidores.

ítem	Descripción	Cantidad	Valor Unitario (USD)	Valor Total (USD)
1	UPS 6 KVA	1	5200	5200
2	Instalación, configuración y capacitación.	8	100[17]	800
Total				6000

Tabla 50. Costo UPS.
Fuente: Departamento comercial empresa distribuidora UPS
Elaborado por el autor

3.2.7 CONTROL DE ACCESO

Al igual que en los demás sistemas como UPS y Cableado estructurado, para el sistema de control de acceso es necesario detallar el costo del sistema, de la instalación y de los accesorios necesarios para el correcto funcionamiento. Ver Tabla 51.

Ítem	Elemento	Cantidad	Costo Unitario (USD)	Costo Total (USD)
1	Sistema de control de acceso	1	820	820
2	Cerradura Electromagnética	1	145	145
3	Instalación, configuración y capacitación	5	80[18]	400
Total				1365

Tabla 51. Costo sistema de control de Acceso.
Fuente: Departamento comercial empresa distribuidora control de acceso
Elaborado por el autor

3.2.8 SISTEMA CONTRA INCENDIOS.

En la Tabla 52, se lista los tanto el sistema de detección de humo, el sistema de extinción de fuego y la instalación y configuración del sistema así como el costo de cada ítem y el costo total

Item	Descripción	Cantidad	Costo Unitario (USD)	Costo Total (USD)
1	Sistema de detección	1	3850	3850
2	Sistema de extinción	1	900	900
3	Instalación, configuración y puesta en marcha del sistema	6	100[19]	600
	Total			5350

Tabla 52. Costo Sistema contra Incendios
Fuente: Departamento comercial empresa distribuidora sistema contra incendios
Elaborado por el autor

[1718] Costo hora/hombre
[19] Costo hora/hombre

3.3 ANÁLISIS DE COSTOS

En la Tabla 53 se encuentra listado el detalle de la oferta y costo para cada sistema, equipo o solución y finalmente el costo total del proyecto.

Descripción	Oferta	Costo total (USD)
Sistema de cableado estructurado	Adquisición de materiales, Instalación y certificación de puntos de red.	6058,45
Equipos de red (switches, AP)	Adquisición de equipos y configuración básica.	1679,03
Firewall IPS/IDS	Configuración de IDS/IPS.	220
Sistema de telefonía IP	Instalación, configuración y pruebas de Elastix.	1440
Teléfonos IP	Adquisición de teléfonos, configuración básica.	6500
Protección de punto finales	Adquisición de licencias, Instalación de software, configuración y capacitación.	3390
Disponibilidad (Respaldo) de información	Adquisición de licencias, Instalación de software, configuración y capacitación.	4048
Sistema de suministro alterno de energía	Adquisición de UPS, configuración y puesta en marcha.	6000
Sistema para control de acceso	Adquisición de elementos, configuración, capacitación y pruebas.	1365
Sistema para control de Incendios	Adquisición de equipos, configuración y puesta en marcha.	5350
Total		36050,48

Tabla 53. Costo total del proyecto.
Elaborado por el autor

Adicionalmente al costo total del proyecto se debe indicar si existen costos adicionales a corto plazo (1 a 3 años) referentes a cualquier dispositivo de red, sistema o solución, estos posible costos se detallan en la Tabla 54.

El soporte técnico que requiera cualquiera de los ítems listados en la Tabla 54 no ha sido considerado como costo a corto plazo ya que este rubro fue incluido en el costo total de cada equipo, solución o sistema.

La licencia de mantenimiento le permite a la empresa poder acceder a nuevas versiones de la solución adquirida y al soporte Técnico directamente con el fabricante.

Descripción	Actividades a corto plazo	Inversión Aproximada	Tipo de inversión
Sistema de cableado estructurado.	No aplica	No aplica	No aplica
Equipos de red (switches, AP)	No aplica	No aplica	No aplica
Sistema de telefonía IP	No aplica	No aplica	No aplica
Teléfonos IP	No aplica	No aplica	No aplica
Protección de punto finales	Renovación de licencia de mantenimiento cada año.	45% del costo de compra	Opcional
Disponibilidad (Respaldo) de información	Renovación de licencia de mantenimiento cada año.	45% del costo de compra	Opcional
Firewall IPS/IDS	No aplica	No aplica	No aplica
UPS	Mantenimiento preventivo cada 6 meses.	Ver Tabla 50. Item. 2	Opcional
Sistema para control de acceso	Mantenimiento preventivo cada 6 meses.	Ver Tabla 51. Item. 3	Opcional
Sistema para control de Incendios	Mantenimiento preventivo cada 6 meses.	Ver Tabla 52. Item. 3	Opcional

Tabla 54. Posibles costos adicionales del proyecto a corto plazo.
Elaborado por el autor

El beneficio de la inversión del costo total del proyecto queda determinado en la reducción de los riesgos a los que está expuesta la información pública y sensible de la empresa, realización de los procesos de negocio en un ambiente más adecuado para las labores de una empresa transnacional. Información proporcionada por la empresa indica que entre el año 2013 y 2014, debido a amenazas tecnológicas como malware, indisponibilidad de servicios, uso

inadecuado de contraseñas, además de falta de energía eléctrica, la empresa KUEHNE+NAGEL división PERECIBLES sufrió pérdidas económicas por alrededor de veinte y cuatro mil dólares (USD. 24000), debido a multas por envíos tardíos, negocios no concretados, pérdida de oportunidades de negocio.

4. CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES.

4.1 CONCLUSIONES.

- La guía para realizar la división lógica de la red corporativa en módulos es uno de los principales beneficios de la utilización de la metodología SAFE Cisco, ya que permite a TI organizar y administrar la red de una manera más proactiva.

- La versatilidad de la norma ISO/IEC 27001:2013 brinda a los encargados de asegurar la información en las empresas, la libertad de adaptar la norma a los requerimientos organizacionales sin que el tamaño de la empresa constituya en un tema demasiado privativo.

- Cualquier toma de decisiones resultado del estudio y aplicación de la norma ISO/IEC 27001 conlleva el compromiso constante de la alta gerencia y de los responsables de las unidades de negocio, incluyendo TI.

- La selección de los objetivos de control y controles que plantea la norma ISO/IEC 27002:2013, puede ser revisada internamente por las partes interesadas en el transcurso del tiempo, es por esto que las empresas pueden adoptar u obviar ciertos controles dependiendo de la situación política, financiera o comercial en la que esta se encuentra.

- Las empresas que actualmente tienen implementado el SGSI o ciertos lineamientos de norma ISO/IEC 27001:2005, no requieren de cambios organizaciones drásticos ni inversiones económicas grandes para adoptar la norma actual.

- El catálogo de amenazas y vulnerabilidades posibilita a los participantes en un proyecto de aseguramiento de la información sensible, aterrizar y contextualizar y adaptar de mejor manera las ideas que se tengan a los requerimientos de la empresa, ya que la identificación de estos factores puede resultar complicado o tedioso.

4.2 RECOMENDACIONES

- Antes de la implementación de normas, políticas, procedimientos para el uso de información sensible de la empresa, es recomendable realizar una charla puntualizando la importancia de la concienciación por parte de los usuarios como el primer paso para el aseguramiento de la información.

- Se recomienda ejecutar los procedimientos para la implementación de controles descritos en el punto 2.3.2.1, además de la difusión oportuna y efectiva de las políticas de control a los distintos actores de los procesos del negocio.

- Dado que las actividades comerciales de la empresa se extienden durante todos los días de la semana, la instalación del cableado estructurado nuevo debería ser programado cuidadosamente o en su defecto éste debería ser paralelo al cableado existente.

- Con las bases planteadas en este proyecto, se recomienda realizar una segunda revisión, a mediano plazo, de amenazas y vulnerabilidades con el fin de considerar la implementación de nuevos controles o la modificación en el alcance de los controles escogidos utilizando la norma ISO/IEC 27002:2013.

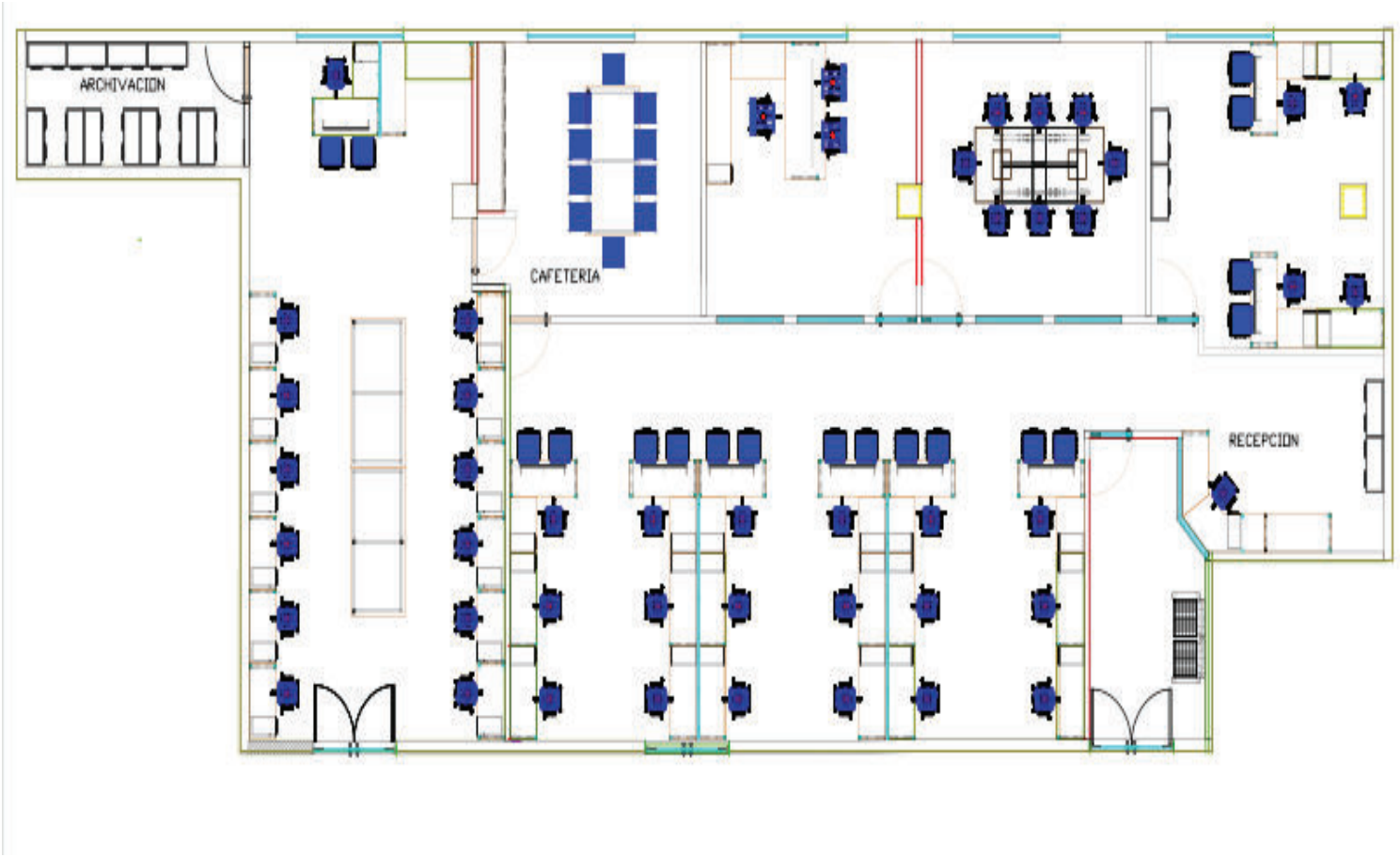
- Se recomienda que la o las empresas que realicen la configuración de la central IP, del servidor de protección de puntos finales, del servidor de

respaldos de información brinden capacitación sobre el uso, configuración y solución de problemas más comunes de cada una de las soluciones, adicionalmente mantener un vigente un contrato en el que se especifique un acuerdo de nivel de servicio acorde a la criticidad de la información que maneja la empresa.

- La tendencia actual “Bring Your Own Device” BYOD “Trae tu propio dispositivo” faculta a las empresas a brindar el servicio de Internet Inalámbrico, es importante comunicar a los usuarios las responsabilidades que conlleva el acceso a este servicio, como el uso principalmente por motivos laborales.

ANEXOS

ANEXO 1. DIAGRAMA DE DISTRIBUCION APROXIMADO DE DISTRIBUCION DE MOBILIARIO



ANEXO 2. ENTREVISTA – TASACION DE ACTIVOS DE INFORMACION

Tasación de activos

Fecha: 11 de Febrero de 2015

Elaborado por:

- Luis Andrés Villavicencio

Participantes:

- Edgar Chicaiza
- Cesar Moya
- Andrés Peñaherrera

Criterios de Tasación:

Los criterios de tasación de la tabla 1 son valores que nos permiten calificar el impacto dentro de un rango controlado: Alto, medio, bajo.

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Tabla 1 Criterios de tasación.

Indicaciones:

Conteste las siguientes preguntas y ubique sus respuestas en la tabla 2.

Preguntas:

¿Cuál es el impacto que tendría para el proceso de "Planificación y Programación" en la organización KUEHNE+NAGEL división PERECIBLES en caso de pérdida de confidencialidad en el activo? Califique tomando los valores de la tabla 1.

¿Cuál es el impacto que tendría para el proceso de "Planificación y Programación" en la organización KUEHNE+NAGEL división PERECIBLES en caso de pérdida de integridad en el activo? Califique tomando los valores de la tabla 1.

¿Cuál es el impacto que tendría para el proceso de "Planificación y Programación" en la organización KUEHNE+NAGEL división PERECIBLES en caso de pérdida de disponibilidad en el activo? Califique tomando los valores de la tabla 1.

Activos	Criterios de Tasación		
	Confidencialidad	Integridad	Disponibilidad
Servidores	2	3	3
Computadores	2	3	3
Teléfonos	1	1	2
Switches	2	3	3
Router	2	3	3
Impresoras	1	1	2
Instalaciones	—	—	3
Aplicación web de facturación	3	3	3
Aplicativo de manejo de reservaciones	3	3	3
Información de clientes	3	2	2
Información de proveedores	2	2	3
Guías de envío	3	3	1
Correo Electrónico	3	3	2
Sistema Operativo	2	3	2

Activos	Criterios de Tasación		
	Confidencialidad	Integridad	Disponibilidad
Personal de Coordinación	—	—	2
Personal de Operaciones	—	—	2
Proveedores	—	—	2

Tabla 2. Tasación de activos

Para constancia de la reunión efectuada firman los asistentes:

Luis Andrés Villavicencio: .....

Edgar Chicaiza: .....

Cesar Moya: .....

Andrés Peñaherrera: .....

ANEXO 3. CATALOGO DE AMENAZAS Y VULNERABILIDADES

CATALOGO DE AMENAZAS Y VULNERABILIDADES		
ACTIVOS	AMENAZAS	VULNERABILIDADES
INFORMACION IMPRESA Y DOCUMENTOS		
	Uso no controlado de datos	Inadecuada clasificación de archivos
	Lectura, copia, remoción no autorizad de documentos archivados	Locación - almacenamiento no protegido
	Degradación de documentos de papel	Locación - almacenamiento no protegido
	Deterioro de medios de almacenamiento	Locación - almacenamiento no protegido
INFORMACION ELECTRONICA – DATOS		
	Acceso con usuario Administrador	Control de acceso inadecuado
	Manipulación – Corrupción de datos inadvertida	Control de acceso inadecuado
	Manipulación – Corrupción de datos deliberada	Control de acceso inadecuado
	Eliminación negligente de datos	Control de acceso inadecuado
	Copia de datos	Control de acceso inadecuado
	Código malicioso	Debilidad o ausencia de protección contra código malicioso
	No disponibilidad de respaldo	Ausencia de políticas de respaldos
SOFTWARE APLICATIVOS DE NEGOCIO		
	Modificación, eliminación de datos por usuario autorizado	Control de acceso inadecuado
	Modificación, eliminación de	Control de acceso

CATALOGO DE AMENAZAS Y VULNERABILIDADES		
ACTIVOS	AMENAZAS	VULNERABILIDADES
	datos por usuario no autorizado	inadecuado
	Lectura o copia de datos	Control de acceso inadecuado
	Falla de aplicativo	Especificación incorrecta o inadecuada
	Exposición de usuario y contraseña	Debilidad en el desarrollo del aplicativo
	No disponibilidad de respaldo	Ausencia de políticas de respaldos
	Interrupción del servicio durante la Instalación/actualización	Control inadecuado de cambios
	Error del aplicativo	Debilidad en el desarrollo del aplicativo
	Error de operación del personal	Falla de capacitación / procedimientos documentados
SOFTWARE STANDARD		
	Uso de software sin licencia	Falta de licencias
	Multas por faltas a la propiedad intelectual	Falta de licencias
	Defectos del software	Falta de testeo de software
	Código malicioso	Antivirus no actualizado o no disponible
	Acceso no autorizado	Inadecuado control de acceso
	Modificación, eliminación de datos por usuario autorizado	Inadecuado control de cambios
	Modificación, eliminación de datos por usuario no autorizado	Inadecuado control de cambios
	Interrupción del servicio durante la Instalación/actualización	Inadecuado control de cambios
	Corrupción de datos	Uso de parches sin testeo
	Explotación de debilidad	Falta de parches

CATALOGO DE AMENAZAS Y VULNERABILIDADES		
ACTIVOS	AMENAZAS	VULNERABILIDADES
	conocida	
HARDWARE		
	Acceso a través de la red por usuario no autorizado	Control de acceso inadecuado
	Acceso físico no autorizado	Control de acceso inadecuado
	Falla/daño en el equipo	Falta de mantenimiento planificado
	Falla suministro eléctrico	Inadecuado suministro de energía
	Código malicioso	Antivirus no actualizado o no disponible
	Modificación / eliminación de datos por usuario autorizado	Inadecuado control de acceso
	Explotación de debilidad conocida	Falta de parches
	Mal uso de puertos de acceso	Inadecuado control de acceso
	Interrupción del servicio durante la Instalación/actualización	Inadecuado control de cambios
	Capacidad de crecimiento de información limitada	
	Descarga no controlada de software	Inadecuado control de acceso
	No disponibilidad de respaldo	Ausencia de políticas de respaldos
COMUNICACIONES		
	Uso no controlado de equipos	Uso no controlado
	Falla en los enlaces de comunicación	Falla de monitoreo
	Defecto en el software (firmware)	Falta de parches
	Acceso físico no autorizado	Inadecuado control de acceso

CATALOGO DE AMENAZAS Y VULNERABILIDADES		
ACTIVOS	AMENAZAS	VULNERABILIDADES
	Falla / daño en el equipo	Falta de mantenimiento
PERSONAS		
	Acceso no autorizado a la información	Debilidad en control de acceso a la información
	Copia no autorizada de información	Ausencia de acuerdos de confidencialidad
	Error en la operación y desarrollo del trabajo	Falta de capacitación
	Ausencia de funcionario	No definición de reemplazos / alternos
	Concentración del conocimiento	No definición de reemplazos / alternos
	Mal uso de recursos	Falta de conciencia de seguridad de la información
	No cumplimiento de perfiles para el cargo.	Debilidad en la definición de puestos y perfiles
INSTALACIONES / SERVICIOS		
	Incendio	Inadecuada prevención / detección de incendios
	Erupción volcánica	Desastre natural
	Bomba	Protección física inadecuada del sitio
	terremoto	Desastre natural
	Falla suministro eléctrico	Planta eléctrica / batería no disponible
	Acceso no autorizado al sitio	Control de acceso inadecuado al sitio
	Acceso a servicios del sitio	Control de acceso inadecuado al sitio

ANEXO 4. ESTRUCTURA DE LA NORMA ISO/IES 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ANEXO 5. CARACTERISTICAS TECNICAS UPS

Computer Power 6/10 KVA Online UPS Selection Guide

MODEL	Computer Power 6K	Computer Power 10K
PHASE	2-phase in / 2-phase out	
CAPACITY	6000 VA / 4800 W	10000 VA / 8000 W
INPUT		
Nominal Input Voltage	208 / 220 / 230 / 240 /VAC; L - L	
Input Voltage Range	80 - 140 VAC / L - N 138 - 242 VAC / L - L; 120°, 240° 160 - 280 VAC / L - L; 180°	
Input Frequency Range	40 Hz - 70 Hz	
Operating Frequency	50 Hz / 60 Hz Auto sensing	
Wiring	L1, L2, N with ground	
Phase Angle	0°/120°/180°/240°	
Power Factor	≥ 0.99 @ 100% load	
OUTPUT		
Nominal Output Voltage	110/115/120/127 VAC (L-N) 200 / 208 / 220 VAC; L - L; 120°, 240° 220 / 230 / 240 VAC; L - L; 180°	
Wiring	L1, L2, N with ground	
Phase Angle	0°/120°/180°/240°	
AC Voltage Regulation (Batt. Mode)	± 1%	
Output Frequency	50 Hz / 60 Hz Auto sensing	
Frequency Range (Batt.Mode)	50 Hz ± 0.1 Hz or 60 Hz ± 0.1 Hz	
Current Crest Ratio	3:1 (max.)	
Harmonic Distortion	≤ 2 % THD	
Transfer Time	Zero	
Waveform	Pure sine wave	
EFFICIENCY		
AC Mode	89%	
Battery Mode	85%	
ECO Mode	96%	
BATTERY		
Nominal Voltage	120 VDC	
Battery Type	12 V / 9 AH	12 V / 7 AH
Numbers	10 pcs x 2 strings	10 pcs x 4 strings external cabinet
Typical Recharge Time	5 hours recover to 90% capacity	7 hours recover to 90% capacity
Float Charging Voltage	136.5 VDC	
Backup Time Full/Half Load	9 / 23 minutes	
INDICATORS		
LCD Display	UPS status, Load level, Battery level, Input/Output voltage, Discharge timer, and Fault conditions	
ALARM		
Battery Mode	Beeps every 4 seconds	
Low Battery	Beeps every second	
Overload	Beeps twice every second	
Fault	Continously sounding	
PHYSICAL		
Dimension,D x W x H(mm)	592 x 250 x 576	592 × 250 × 626
Net Weight (kgs)	53 Kg	UPS: 35 Kg / Batt cabinet: 109 Kg
ENVIRONMENT		
Operational Humidity and Temperature	0-95 % RH @ 0- 40°C (non-condensing)	
Noise Level	Less than 60dBA @ 1 Meter	
Operational Altitude	≤ 3000 meters	
MANAGEMENT		
Smart RS-232 / USB	Supports Windows® 2000/2003/XP/Vista/2008, Windows® 7, Linux, Unix, and MAC	
Optional SNMP	Power management from SNMP manager and web browser	

Bibliografía

Proyectos de titulación

- DISEÑO DE LA RED PARA VOZ Y DATOS, ACCESO REMOTO E INTRANET PARA LA EMPRESA ACURIO&ASOCIADOS.
  Autor: Williams David Leiva Pacheco/Andrea Isabel Muñoz Parreño
  Año y lugar: Quito/ EPN/2011.

- DISEÑO DE LA RED DE TELEFONIA IP Y SU INTEGRACION CON LA RED DE DATOS PARA LA COMUNICACIÓN DE LA MATRIZ CON LAS SUCURSALES DE LA IMPORTADORA VEGA S.A.
  Autor: Aveiga Lovato, Diana Cristina/ Cadena Lozano, Luis Alfredo
  Año y lugar: Quito /EPN/2010

- DISEÑO DE LA RED DE CORPORATIVA DE VOZ Y DATOS PARA EL SERVICIO ECUATORIANO DE CAPACITACION PROFESIONAL (SECAP)
  Autor: Sandoval Abad Mireya Soledad/ Vera Cueva, Johanna Elizabeth
  Año y lugar: Quito /EPN/2012

- ELABORACION DEL PLAN DE SEGURIDAD DE LA INFORMACION PARA EL FONDO DE CESANTIA Y JUBILACION DEL MDMQ
  Autor: Abalco Maila David Elias / Ruilova Sandoval Romel Ruperto
  Año y lugar: Quito /EPN/2014

Normas

- SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks.

- Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013

- Information technology – Security techniques – Code of practice for information security control

Páginas Web

- Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002.
  http://iso27000.es/iso27002.html

- ¿Qué es Norma ISO 27001?
  http://www.iso27001standard.com/es/que-es-iso-27001/

- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
  http://www.iso27001security.com/html/27002.html

- Voice over Internet Protocol
  http://www.phonet.cz/archiv/dok_cizi/ieeeespectrumVoIP.pdf

- Network Design: Firewall IDS/IPS
  http://resources.infosecinstitute.com/network-design-firewall-idsips/

- Elastix Virtualizado
  http://elastixtech.com/elastix-virtualizado/

- ISO/IEC 27001:2013
  http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/

- Voz sobre IP: Performance Evaluation on VmwareVsphere 5
  http://www.vmware.com/files/pdf/techpaper/voip-perf-vsphere5.pdf

Apuntes:

Curso – Taller Intensivo ISO/IEC 27001:2013. Dictado por ISEC Ecuador
Septiembre 2014