UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIONES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

AUDITORÍA DE SISTEMAS INFORMÁTICOS

PRESENTADO POR

BACHILLER JORGE WALTER ALFARO SOTO

ASESOR

ING. WALTER DEMETRIO COAYLA MAMANI

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

MOQUEGUA – PERÚ

2019

CONTENIDO.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

CONTENIDO DE TABLAS

Pág.

CONTENIDO DE FIGURAS

Pág.

CONTENIDO APÉNDICES

RESUMEN

El trabajo que se presenta describe la aplicación de una auditoría informática, lógica y física a la empresa OK Computer EIRL, utilizando COBIT como marco de trabajo. Se evidenciaron problemas que evidencia la vulnerabilidad en la seguridad que exponían la integridad de la información en la empresa. Finalmente se realizaron recomendaciones para corregir los problemas y asegurar el correcto funcionamiento de la empresa. La auditoría informática es importante en la empresa para evaluar si las herramientas utilizadas sacan el máximo partido a la actividad empresarial y si la información que se maneja se encuentra segura y protegida.

Palabras clave: Auditoria, seguridad, información, vulnerabilidad.

ABSTRACT

This work describes the application of an informatics, physical and logical audit to the enterprise OK Computer EIRL, using COBIT as a framework. There were security problems that exposed the integrity of the company's information. Finally, recommendations were made to correct those problems and ensure the proper functioning of the company. The computer audit is important in the company to evaluate if the tools used make the most of the business activity and if the information that is handled is safe and protected.

Keywords: Audit, security, information.

CAPÍTULO I

INTRODUCCIÓN

El documento que se presenta propone el cumplimiento de una auditoría lógica y física a la empresa OK Computer EIRL, que se dedica al rubro de tecnologías de la información. La empresa se dedica a ofrecer soluciones generales de software, hardware y servicios. El portafolio de las actividades que realiza es de diversos tipos como networking, telefonía, data center, infraestructura, red de acceso, soluciones inalámbricas, asesoramiento en elaboración y ejecución de proyectos tecnológicos, licenciamiento de software y equipamiento tecnológico.

Por lo tanto, se pretender utilizando como base la auditoría informática, determinar cada uno de los procesos del negocio con el fin de identificar las fortalezas y debilidades en la gestión de los procesos que realiza la empresa.

Durante la ejecución de la auditoría se realizaron evaluaciones, para poder identificar el nivel de seguridad, planificación y eficacia con que se están rigiendo los procesos existentes de la empresa.

Con la información obtenida durante la auditoría se desea mejorar los procesos obtenidos que muestran debilidad en la revisión y evaluación de los controles, comunicación, sistemas y procedimientos de la empresa. Al terminar el proceso de auditoría informática se pretender poner en práctica las

Recomendaciones por lo que se pretende optimizar la eficiencia y seguridad de la información obtenida por la empresa, como también los métodos para la toma de decisiones.

CAPÍTULO II

OBJETIVO

2.1. Objetivo general

Realizar un plan de auditoría lógica y física de los sistemas de información y tecnología de comunicación de la empresa OK Computer EIRL

2.2. Objetivos específicos

Comprobar la existen de controles en la empresa OK Computer.

Aplicar técnicas de auditoría informática para la evaluación de controles enfocados en los riesgos informáticos.

Presentar un informe de hallazgos como resultado de la auditoría con resultados y recomendaciones.

CAPÍTULO III

DESARROLLO DEL TEMA

Al realizar la auditoría a la empresa Ok Computer EIRL se podrá valorar el manejo y la eficiencia de la información y el desarrollo de los procesos de la empresa, por lo que se requiere vigilar en todo momento los procesos de recopilación, procesamiento y almacenamiento de la información de la empresa, para tal caso nos apoyaremos del uso de las tecnologías informáticas, en cualquier empresa el desarrollo de estos procesos es vital para su correcto desempeño de la empresa.

Una vez culminado el informe de análisis del proceso de auditoría, la alta gerencia podrá tomar decisiones para que pueda mejorar su el rendimiento de su red física y el uso de sistemas de información ya que esto les podrá ayudar en mejorar los procesamientos de información, permitiendo mejorar la atención a los clientes.

También podremos decir que al ejecutar esta auditoría la empresa tendrá identificado todo el peligro de los procesos informáticos, comprobando su calidad y capacidad a cuanto a las peticiones de hardware y software.

3.1. Marco teórico

Al iniciar se hará un análisis teórico referente a la auditoría, los objetivos, definición, importancia, tipos, controles, riesgos, controles internos, metodología, tipos de herramientas, funciones, planeación de la auditoría, finalizando con un informe de auditoría

3.1.1. Generalidades de la auditoría.

La auditoría tiene como principal función apoyo en la dirección, la cual tiene como finalidad de analizar y apreciar el control interno de las empresas, a través de vistas a las eventuales operaciones correctivas que sirven para garantizar la integridad de su patrimonio, la integridad de la información y el mantenimiento de la eficacia de sus sistemas de gestión.

La ejecución de una auditoría siempre debe de ser de carácter independiente, no es de carácter ejecutivo ni son vinculantes sus conclusiones, la organización puede decidir qué acciones quedan pendientes.

La finalidad de la auditoría es el uso adecuado de la información dentro del ámbito de la empresa, y entregar oportunamente los resultados a la organización, incluyendo todas las evaluaciones del cumplimiento de funciones, actividades y operaciones que realicen los empleados y usuarios de la empresa.

La auditoría nace en relación que el comercio tiene un crecimiento bastante amplio, es entonces que surge la necesidad de revisiones para garantizar el correcto proceso de manejo de procesos de la organización. La auditoría como tal fue reconocida por primera vez en las leyes británicas de sociedades anónimas en 1862 y fue reconocida durante el mandato de ley.

3.1.2 Tipos de auditoría.

La auditoría tiene gran importancia para el eficiente funcionamiento de una organización para poder entenderla ha sido necesario dividirla de acuerdo el tipo de área a trabajar, con la finalidad de mejorar los análisis al momento de comenzar los trabajos.

3.1.2.1. Auditoría externa.

Es aquella que se ejecuta con una empresa externa de profesionales, con el propósito de calificar los estados financieros de la organización. Es un proceso normal cuando se desea señalar que una organización se conduce de forma honesta.

3.1.2.2. Auditoría financiera.

Tiene como principal finalidad evaluar los estados financieros de la organización por un auditor el cual trabajo la información contable, con el propósito de poner en conocimiento los resultados de su trabajo.

3.1.2.3. Auditoría fiscal.

Es un trabajo que tiene como finalidad evaluar y obtener evidencias cerca de hechos que se vinculan con acciones de carácter tributario.

3.1.2.4. Auditoría integral.

Es un trabajo más crítico, detallado y sistemático de los sistemas de información financieros, de gestión y legales de la organización. Realizado de forma autónoma y usando técnicas detalladas, con la finalidad de mostrar un informa detallado con la racionalidad del estado de información financiera.

La eficiencia, eficacia y economicidad del manejo de los recursos y apego a las operaciones económicas a las normas contables con el fin de tomar decisiones que mejoren la productividad de la empresa.

3.1.2.5. Auditoría interna o de campo.

La auditoría de campo es un trabajo que cae como responsabilidad en la gerencia de las organizaciones, y esta conceptuada para dar seguridad sobre los logros de los objetivos de la empresa.

3.1.2.6. Auditoría interna o auditoría contable financiera.

Es una auditoría que tiene como principal funciona averiguar a detalle y autenticidad los estados financieros y otros documentos de carácter administrativo y contable, los cuales fueron entregados por la dirección.

3.1.2.7. Auditoría informática

La auditoría informática, es el resultado de recoger, evaluar y agrupar evidencias para resolver si un sistema de información guarda el activo empresarial, conserva la integridad de los datos, maneja eficazmente los fines de la empresa, lleva eficientemente los recursos y si trabaja con las leyes de regulación establecidas (Ramírez, 2009, p. 14)

Durante los trabajos de una auditoría lo primordial es evaluar los mecanismos de control que están definidos en una organización, revisando si estos son los adecuados y si cumplen determinados objetivos y estrategias ya definidas, (Ramírez, 2009, p. 14)

3.1.3. COBIT 4.1.

COBIT (Control Objetive for Information and Related Technology) son los lineamientos aceptados a nivel internacional como buenas prácticas, para el

control de la información en TI y los riesgos que llevan, COBIT es una herramienta utilizada para implementar el gobierno de TI y optimizar los controles de TI. Contiene objetivos de control, reglas de seguimiento, medidas de desempeño, factores críticos y de éxito y guías de madurez.

COBIT es marco de trabajo de gobierno de TI y un grupo de herramientas que dan soporte al gobierno de TI. Esto les da a los gerentes una herramienta la cual les ayuda a cubrir las brechas entre los requerimientos del control, los aspectos técnicos y los riesgos que tiene el negocio.

Gracias a COBIT es que se hace posible un desarrollo de una política más clara y de buenas prácticas los cuales ayudan los controles de TI a través de las organizaciones.

COBIT enfatiza en la conformidad de regulaciones, colabora con las organizaciones a incrementar el valor alcanzado desde las TI, también permite el alineamiento y reduce la implementación de las estructuras COBIT

3.1.3.1. Misión.

La misión de COBIT es desarrollar, investigar promover y publicar un conjunto de normas internacionales autorizadas y actuales, de objetivos que tengan el manejo de las tecnologías de información aceptados por lo general por el uso de gerentes de organizaciones de auditores.

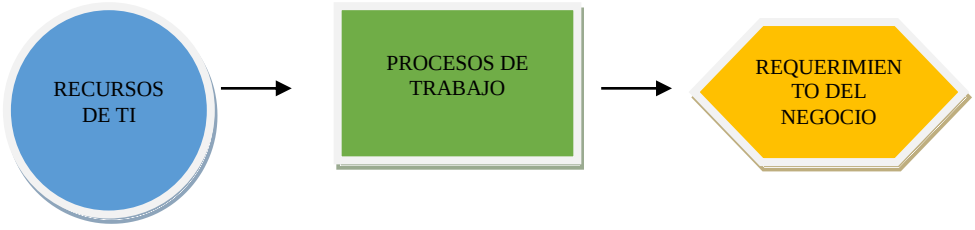
La función de COBIT es de entregar una guía estándar que tenga aceptación internacional sobre los objetivos de control que deben actuar en un ambiente de tecnologías de información, con el fin de asegurar que las

organizaciones puedan llegar a sus objetivos de su negocio y que dependan del buen uso de la tecnología.

3.1.3.2 Estructura.

COBIT alcanza un acercamiento en el ámbito de negocios y en las tecnologías de información en los ámbitos que eran alejados uno del otro, y que eran necesarios que se unan.

La idea de COBIT son que lo medios de TI se utilicen de manera adecuada con procesos de trabajo, para poder lograr cumplir los requerimientos de información que la organización así lo exija. Tal como se muestra en la figura 1 estructura del estándar de cobit 4.1.



- Datos
- Sistema de información
- Tecnología
- Instalaciones
- Recursos humanos

- Planeamiento y organización
- Adquisición e implementación
- Prestación de servicios y soporte
- Monitoreo

- Efectividad y eficiencia
- Confidencialidad
- Integridad y disponibilidad
- Confiabilidad de la información
- Cumplimiento de leyes y regulación

Figura 1. Estructura del estándar de cobit 4.1

3.1.3.4 Recursos de TI

COBIT se clasifica sobre los recursos tecnológicos de la siguiente forma

- **Datos:** Son todas las formas de información en sentido más pleno, se considera la información interna y externa estructurada, no estructurada, sonido, gráfica.

- **Sistemas de información:** Son los sistemas o aplicaciones que trabajan tanto en procedimientos programados como procedimientos manuales.
- **Tecnología:** Incluye todo tipo de tecnología, sistemas operativos, hardware, software, equipos de telecomunicación, redes, video, etc.
- **Instalaciones:** Son los recursos de la empresa necesarios que sirven para dar soporte a los sistemas de información.
- **Recursos humanos:** Son todas las habilidades, productividad del personal que sirven para adquirir, planear, adquirir servicios, dar soporte y supervisar los sistemas y servicios.

3.1.3.5 Proceso de Trabajo.

Los dominios establecidos en COBIT están estructurados de acuerdo con el esquema de ciclo de vida de administración de recursos los cuales son:

- Planeación y Organización (PO)
- Adquisición e implementación (AI)
- Entrega de servicios y soporte (DS)
- Monitoreo (M)

Estos dominios también se dividen en subprocesos.

a. Planeación y organización (PO).

P01 Definir un plan estratégico de sistemas.

P02 Definir las arquitecturas de información.

P03 Definir la dirección tecnológica.

P04 Definir la dirección Tecnológica.

P05 Administrar las inversiones de TI.

P06 Comunicar la dirección y objetivos de la gerencia.

P07 Administrar los recursos Humanos.

P08 Asegurar el apego a disposiciones externas.

P09 Evaluar riesgos.

P010 Administrar proyectos

b. Adquisición e implementación (A).

AI1. Adquirir y mantener software de aplicaciones.

AI2. Adquirir y mantener software de aplicaciones.

AI3. Adquirir y mantener la arquitectura tecnológica.

AI4. Desarrollar y mantener procedimientos.

AI5. Instalar y acreditar sistemas de información.

AI6. Administrar cambios.

c. Prestación y servicios de soporte (DS).

DS1. Definir niveles de servicios.

DS2. Administrar servicios

DS3. Administrar desempeño y capacidad.

DS4. Asegurar la continuidad del servicio.

DS5. Garantizar la seguridad del sistema.

DS6. Identificar y asignar costos.

DS7. Educar y capacitar usuarios.

DS8. Apoyar y orientar a clientes.

DS9. Administrar la configuración.

DS10. Administrar problemas e incidentes.

DS11. Administrar la información.

DS12. Administrar las instalaciones.

DS13 Administrar las operaciones.

d. Monitoreo (M).

M1. Monitorear el proceso.

M2. Evaluar lo adecuado del control internet.

M3. Obtener aseguramiento independiente.

M4. Proporcionar auditorías independientes.

3.1.3.6. Requerimientos del negocio.

Con respecto a COBIT los requerimientos del negocio se dirigen en forma exclusiva a los requerimientos relacionados a la informática.

a. Requerimientos de calidad.

- Calidad.
- Costo.
- Prestación de servicios.

b. Requerimientos de confianza.

– Efectividad y eficiencia en operaciones.

– Confiabilidad de la información.

– Cumplimiento de leyes y regulaciones.

c. Requerimientos de seguridad en información.

– Confidencialidad

– Integridad

– Disponibilidad

3.2. Caso práctico

El proceso de auditoría que se aplicó a la empresa OK Computer EIRL se desarrolló empleando COBIT, el cual proporciona una cadena de pasos que sirven como guías para realizar el proceso de evaluación, se trabajó en las diferentes áreas de la empresa, seleccionando el lugar donde se realizaría los procesos informáticos.

3.2.1. Preliminar.

OK Computer EIRL es una empresa que se dedica a integrar tecnología de la información inicia sus actividades el 22/04/2004 y cuenta con más de 15 años de experiencia. En las siguientes áreas:

- Networking
- Colaboración, telefonía, telemedicina
- Data center, virtualización de servidores
- Infraestructura, cableado estructurado
- Red de acceso, fibra óptica, planta externa
- Soluciones inalámbricas WAN y LAN
- Seguridad, video vigilancia, automatización
- Protección electica
- Soluciones interactivas
- Licenciamiento de software
- Equipamiento tecnológico, impresión, suministros
- Leasing, outsourcing, arrendamiento financiero
- Asesoramiento y elaboración de proyectos tecnológicos

La empresa cuenta con diferentes áreas, las cuales son contabilidad, proyectos, administración, almacén y comercial.

Todas las áreas están interconectadas por una red interna propia de la empresa la cual brinda conexión a los servicios de internet e intercomunicación entre los mismos. Tal como se muestra en la figura 2 organigrama de la empresa.

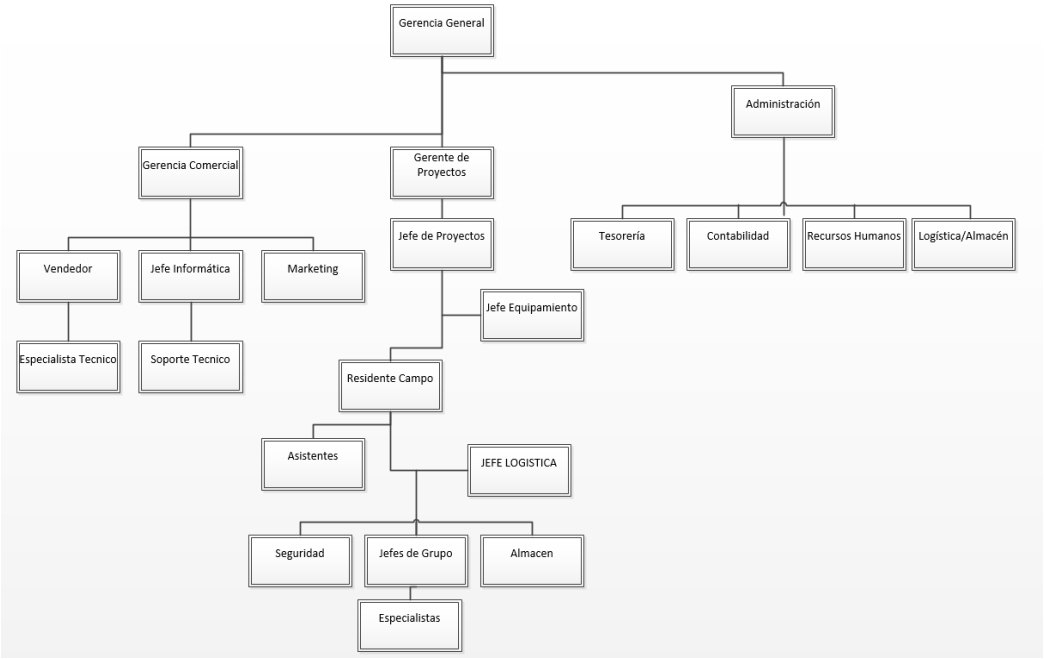


Figura 2. Organigrama de la empresa

Las oficinas cuentan con 25 empleados quienes hacen uso de los equipos informáticos que posee la empresa. Entre los empleados existe un encargado de soporte quien está encargado del manejo del uso de hardware y software.

El área comercial es donde se hace mayor uso de tecnologías de información. Aquí se manejan los dos sistemas importantes para los negocios de la empresa, los cuales son SEACE y SoftLink. Tal como se muestra en la figura 3 y figura 4.

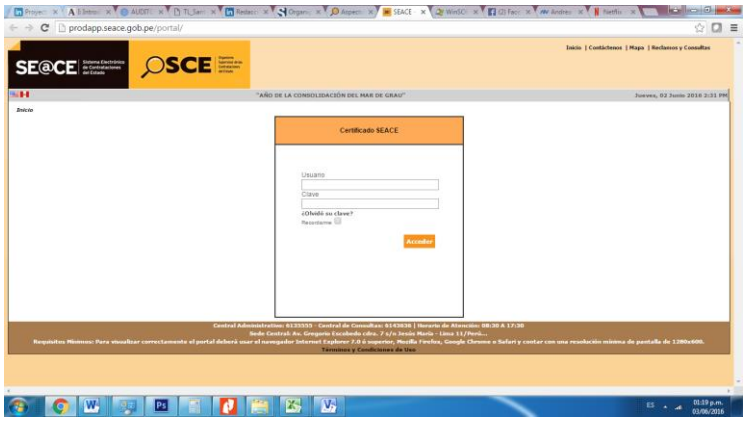


Figura 3. Sistema SEACE

Figura 4. Sistema SoftLink

3.2.2. Justificación.

Con la realización del trabajo de auditoría a la empresa OK COMPUTER EIRL se podrá evaluar el manejo de la información y los métodos que utiliza la empresa, es por ello que se requiere vigilar los procesos de recopilación, almacenamiento y los procesos de información dentro de la empresa, todo esto a través de las tecnologías informáticas .

Teniendo en consideración la evaluación inicial de la empresa se ha decidido que el área a auditar será el área comercial.

3.2.2.1. Gestión de riesgos.

Para la gestión de riesgos se requiere concienciación de los riesgos por la alta gerencia una clara compresión de la empresa para el apetito de riesgo, transparencia acerca de los altos importantes riesgos de la empresa y la incorporación de gestión de riesgo responsabilidades de la empresa. Como muestra la figura 5 área comercial

Figura 5. Área comercial

3.2.2.2. Áreas a auditar

a. Seguridad Lógica.

Verificar la presencia de alguna normativa y procedimientos que sirvan para resguardar el acceso a la información y los permisos de acceso a personal no autorizado.

Tabla 1

Componentes de la seguridad lógica

Componente	Riesgo
Acceso de los usuarios a los sistemas operativos, sistemas y base de datos	Alto
Acceso a los usuarios a programas y archivos	Alto
Disposición de sistemas alternos	Alto
Presencia de software de protección	Alto

b. Seguridad Física.

Se desea valorar la seguridad física de los datos, programas, instalaciones, equipos de red y personal de la empresa.

Tabla 2

Componentes de la seguridad física

Componente	Riesgo
Control de Acceso de los usuarios a los equipos	Alto
Informes de accesos y visitas a las instalaciones	Alto
Inventario de equipos de hardware y software	Alto
Revisión de la red informática	Alto
Controles para la instalación y uso de dispositivos externos	Alto

c. Respaldo y plan de contingencia.

Constatar si se tiene respaldos de información, vitar para el correcto funcionamiento de la empresa, tanto en forma digital como en formato físico, los que deben cumplir los requisitos adecuados.

Tabla 3

Componentes de respaldo de contingencia

Componente	Riesgo
Respaldo de información.	Alto
Plan de continuidad.	Alto
Plan de contingencia.	Alto
Plan de mantenimiento de software y hardware.	Medio

d. Documentación de hardware y software.

Verificar la presencia de documentos de todo lo comprado por la empresa en materia de informática como manuales, contratos, facturas adicionalmente de documentos en donde se detalle los sistemas que la empresa ha adquirido.

Tabla 4

Componentes de documentación de hardware y software

Componente	Riesgo
Disposición de manual de usuario y de instalación de sistema.	Medio
Existe documentación de adquisición de equipos de hardware, software, contratos legales.	Alto
Documentos de los sistemas usados por la empresa.	Alto

3.2.3. Adecuación.

Durante la realización de esta auditoría se han trabajado con diferentes técnicas de recopilación de datos, por medio de las que se pudo obtener información que se necesita para su posterior procesamiento. Las técnicas utilizadas fueron las siguientes:

- Cuestionarios

Son preguntas ordenadas que sirven para obtener información de quien las responde.

- Entrevistas

Es una actividad que realiza el auditor, en esta se logra reunir mayor información con detalle de quien la proporciona por medios puramente técnicos a diferencia de las respuestas planas de los cuestionarios.

– Observaciones

Es una forma de tomar registros de manera visual, en una situación real, se consignan los datos en un esquema ya visto y acorde al problema que se trata.

3.2.4. Guía de auditoría.

Tabla 5

Acceso a los usuarios a sistemas, sistemas operativos y base de datos.

Guía de auditoría	
Dominio	Entrega Servicio y Soporte
Proceso:	DS5. Garantizar la seguridad del sistema
Objetivo	Notar la implementación de controles adecuados para el ingreso de los usuarios.
1	Solicitar al encargado la lista de usuarios que tienen acceso a los sistemas usados en los equipos.
2	Verificar si existe una cuenta de usuario por persona en cada equipos
3	Observar cuantos son los usuarios que cuenta con acceso a los sistemas SEACE, SoftLink y base de datos de la empresa.

Tabla 6

Acceso de los usuarios a programas y archivos.

Guía de auditoría	
Dominio	Entrega de servicio y soporte (DS)
Procesos	DS11 administrar la información.
Objetivo	Verificar que se apliquen normas de acceso a los usuarios al momento de modificar archivos o manipulación de programas propios de la empresa.
1	Observar si los usuarios tienen acceso a la información almacenada en los equipos sin ninguna restricción.
2	Verificar la existencia de medidas de restricción a los usuarios en el uso de archivos en el ordenador, así mismo ver si existe manipulación a programas

Tabla 7

Disposición de sistemas alteños en caso de fallos

Guía de Auditoría	
Dominio	Entrega de servicios y soporte (DS)
Proceso	DS3 Asegurar la continuidad de servicios
Objetivo	Obtener un plan de contingencia si existiera, en caso que los sistemas principales fallen
1	Aplicar entrevistas al encargado del área para conocer con qué medidas cuentan en caso que falle uno de los sistemas
2	Verificar la existencia de servidor alterno donde se almacene la información de clientes y gestión diaria

Tabla 8

Existencia de software de protección (antivirus, firewall)

Guía de auditoría	
Dominio	Entrega de servicios y Soporte (DS)
Proceso	DS3 Asegurar desempeño y capacidad.
Objetivo	Ver el tipo de software y licencias obtenidas, el desempeño y que sean acorde con el tipo de la empresa.
1	Verificar mediante la observación la presencia de software que proteja cada uno de los equipos.
2	En el caso que se encuentre un software verificar si esta actualizado

Tabla 9

Control de acceso de los usuarios a los equipos

Guía de Auditoría	
Dominio	Adquisición e implementación (AI)
Procesos	AI3 Adquirir y mantener la arquitectura tecnológica
Objetivo	Verificar los normativos de uso y acceso a los equipos
1	Solicitar al encargado del área la lista de equipos que se usan, cuantos usuarios las usan y cuantas horas al día son usadas

Tabla 10

Informe de acceso y visita de las instalaciones

Guía de auditoría	
Dominio	Entrega de servicios y soporte (DS)
Procesos	DS12 Administrar las instalaciones
Objetivo	Verificar si existe un control a las visitas a los ambientes informáticos
1	Observar los mecanismos y sistemas de seguridad con respecto al ingreso del área de operaciones, mediante el proceso de operación directa.

Tabla 11

Control de acceso de los usuarios a los servicios de internet

Guía de auditoría	
Dominio	Entrega de servicio y soporte (DS)
Proceso	DS9. Administrar la configuración
Objetivo	Verificar si existen controles para el uso de internet.
1	A través de las entrevista al personal encargado del área, se pretende conocer si dentro de la empresa se tiene algún reglamento del uso del servicio de internet para los usuarios que hagan uso del servicios.
2	Si existe algún reglamento para el uso del servicio, verificar si las reglas son las adecuadas para el óptimo uso del servicio.

Tabla 12

Inventario de equipos y software

Guía de auditoría	
Dominio	Adquisición e implementación (AI)
Proceso	AI3. Adquirir y mantener la arquitectura tecnológica.
Objetivo	Verificar si la empresa cuenta con un inventario y corroborar la información del inventario con lo que existe en la empresa.

Tabla 12

Inventario de equipos y software *(continuación)*

1	Realizar entrevistas al encargado del área con el fin de tomar conocimiento sobre la existencia de algún inventario de equipos y software de respaldo en el caso que algo falle.
2	Si existiera algún inventario verificar su existencia visitando el lugar en donde se almacenan las cosas.

Tabla 13

Revisión de la red factor ambiental, físico y humano.

Guía de auditoría	
Dominio	Entrega de servicios y soporte (DS)
Procesos	Protección contra factores ambientales
Objetivo	Verificar la red física, la disposición que tienen los equipos conectados y todos los usuarios que ingresan a la red.
1	Revisar mediante la observación directa las instalaciones de red y de los equipos para ver si su implantación es de manera correcta

Tabla 14

Controles para la instalación y uso de dispositivos externos.

Guía de auditoría	
Dominio	Entrega de servicios y soporte (DS)
Proceso	DS9 Administrar la configuración
Objetivo	Verificar si existe algún control para el uso de periféricos las restricciones y su alcance
1	Aplicar entrevista al encargado del área para verificar si es que se utiliza algún método en los equipos para poder restringir el acceso a dispositivos externos o si bien existen algún reglamento para el uso de estos mismos.

Tabla 15

Respaldo de información critica

Guía de auditoría	
Dominio	Entrega de servicios y soporte (DS)
Proceso	DS11 Administrar la información
Objetivo	Verificar si existen respaldos de la información vital de clientes y procesos importantes para la empresa
1	Aplicar entrevistas para poder conocer si existen respaldos de la información que se usen en las gestiones diarias
2	Si existen respaldos, verificar de qué tipo de respaldos son ya sean digitales o físicos, si son digitales en que se están almacenando si es por un servidor alterno o discos o memorias

Tabla 16

Plan de continuidad

Guía de auditoría	
dominio	Entrega de servicios y soporte (DS)
Proceso	DS4 Asegurar la continuidad del servicio
Objetivo	Comprar si existe algún plan de continuidad el cual se use en caso de desastres naturales o accidentes provocados por la naturaleza humana y que pueda detener totalmente las operaciones de la empresa
1	Realizar entrevistas al encargado del área de soporte para así conocer si cuentan con algún plan de continuidad ante un desastre natural o causado por personas que pueda detener totalmente las operaciones
2	Si este plan existe solicitar los detalles mínimos de este y de los pasos que se realizarían al momento de que se presente un caso de estos que pueda detener las operaciones totales de las operaciones

Tabla 17

Plan de contingencia

Guía de auditoría	
Dominio	Entrega de servicios y soporte(DS)
Procesos	DS4 Asegurar la continuidad del servicio
Objetivo	Determinar si el plan de contingencia es suficientemente detallado para poder continuar con los trabajos de la empresa y que adicionalmente, dicho plan este de acuerdo a lo que la empresa tienen en sus recursos(
1	Realizar entrevistas al encargado del área de mantenimiento para conocer si existe un plan de contingencia al momento de un fallo.
2	Si existiera el plan de contingencia, pedir los detalles de que se realizaría si en el momento que se presente algún fallo que detenga parcialmente los trabajos

Tabla 18

Plan de mantenimiento de hardware y software

Guía de auditoría	
Dominio	Adquisición e implementación (AI)
Proceso	AI3 Adquirir y mantener la arquitectura tecnológica
Objetivo	Revisar el plan de mantenimiento de software, si el periodo entre cada mantenimiento es el adecuado y si se hace el mantenimiento adecuado
1	Verificar la existencia de un plan de manteniendo a través de entrevista al encargado del área de mantenimiento
2	Si este plan existe, conocer qué tipo de plan se tiene y que detalles abarca el mismo para el mantenimiento de equipos y software en general de la empresa.

Tabla 19

Disposición de manuales de usuario y de instalación de los sistemas

Guía de auditoría	
Dominio	Adquisición e implementación (AI)
Proceso	AI2 Adquirir y mantener software de aplicaciones

Tabla 19

Disposición de manuales de usuario y de instalación de los sistemas (continuación)

Objetivo	Revisar los manuales de usuarios de los software que están actualmente en uso y si estos manuales se encuentran actualizados
1	Solicitar al encargado los manuales de usuario de los sistemas que utilizan para la gestión de servicios que la empresa utiliza
2	Verificar los manuales para observar si son acordes a la versión del software que se está usando

Tabla 20

Existencia de documentos de adquisición de equipos, software y contratos legales de proveedor de internet

Guía de auditoría	
Dominio	Adquisición e implementación (AI)
Proceso	AI3 adquirir y mantener la arquitectura tecnológica
Objetivos	Verificar las compras de equipos mediante documentos legales(facturas) y verificar el contrato de internet ISP para poder determinar lo estipulado en el contrato y verificar su correcto funcionamiento
1	Solicitar al encargado del área de adquisición el registro o respaldo de facturas donde se demuestre la adquisición de equipos, software o servicios

Tabla 21

Documentación de los sistemas utilizados para los servicios de la empresa

Guía de auditoría	
Dominio	Adquisición e implementación(AI)
Procesos	AI2 adquirir y mantener software de aplicación
Objetivo	Verificar si existe la documentación de los sistemas adquiridos por la empresa y si esta posee todos los aspectos necesarios para poder dar manteamiento al sistema en caso de ser necesario

Tabla 21

Documentación de los sistemas utilizados para los servicios de la empresa (continuación)

1	Mediante las entrevistas conocer si la empresa al adquirir un sistema obtiene la documentación del mismo como diagramas, arquitectura, código, etc. para poder ser modificados

3.2.5. Formalización.

Se formalizó la ejecución de la auditoría en una reunión con la dirección de la empresa, donde se llegó a un acuerdo entre el gerente general y el auditor para definir el área de la auditoría definir los limites, alcances, las visitas y tiempo que durara la evaluación.

3.3. Representación de resultados.

3.3.1. Seguridad física.

Tras verificar los módulos descritos en la seguridad física, se pudo observar los siguientes hallazgos, los cuales se detallan a continuación:

3.3.1.1. Control de acceso de los usuarios a los equipos.

Se pudo observar que los usuarios que laboran en las oficinas administrativas cuentan con acceso a los equipos

Poder contar con controles hacia el ingreso de equipos, evita la exposición tanto de la información como de los equipos por riesgos ocasionados por accidentes o acciones del personal generando mayores garantías de la disponibilidad e integridad de la información.

3.3.1.2. Informe de acceso y visitas a las instalaciones.

Se pudo apreciar que la organización no cuenta con un registro de control de ingreso al edificio. Las notificaciones para ingresar al edificio se hacen de manera

verbal, además al ingresas a la empresa, ningún personal solicita alguna identificación a la persona ingresante, únicamente se pregunta hacia donde se dirige el visitante y a quien busca, se cuenta con una cámara de seguridad para registrar el acceso

Poder contar con un registro de visitantes, personal externo en una empresa es importante, ya que de esta manera se podrá contar con un ambiente seguro para el personal que labora en la empresa. También se protegen los activos, continuidad operacional y la propiedad intelectual de la empresa. Figura 6 cámaras de seguridad ubicada en puerta de ingreso

Figura 6. Cámara de seguridad ubicada en la puerta de ingreso de la empresa

3.3.1.3. Inventario de equipos y software.

Con respecto al inventario de equipos y software de la empresa, se pudo observar que la empresa cuenta con un sistema de almacén donde se encuentran los equipos informáticos y electrónicos operativos y no operativos. Se tiene un inventario realizado de forma manual, en donde se guarda la información de los equipos y su estado de operatividad,

En el software SoftLink se cuenta con un módulo de almacén, donde el jefe de logística lleva un control del patrimonio de los equipos de la empresa.

Es de vital importancia que la empresa cuenta con un inventario de hardware y software al día, de tal modo que la empresa cuenta con un control directo de todos sus activos de TI y saber exactamente con lo que se cuenta almacenado y comprar lo necesario en caso que se tenga alguna venta.

3.3.1.4. Revisión de la red (factor ambiental, físico y humano).

La red de la empresa esta generalmente compuesta por cableado plano, el ISP (movistar), les proporciona un servicio dúo con acceso a internet de 8Mbps, esta línea se conecta a un Router proporcionado por el ISP ubicado en la oficina de almacén en un gabinete de 24RU de piso cerrado con llave, y como respaldo eléctrico tienen un UPS de autonomía de 2 horas. Figura 6 cableado de red en un gabinete

Figura 6. Cableado de red en un gabinete de la empresa

La red de la empresa se divide en cuatro sub-redes las cuales son;

- Telefónica IP
- Administración
- Área comercial
- Área de proyectos

En la red, el cableado UTP va a través de canaletas hasta llegar a los equipos, en donde es conectado directamente al puerto de red del ordenador. Ningún punto de datos cuenta con un faceplate. Se pudo evidenciar que el único estándar para el cableado estructurado que se cumple en el transcurso de trasmisión de datos es EIA/TIA. Por otro lado, la empresa también cuenta como backup un sistema de inalámbrico para algunos trabajadores a través de Access Point los cuales están ubicados en el área comercial y en el área de administración. Ambos equipos poseen la seguridad de filtrado por MAC y clave WPA.

Cabe señalar en relación a la seguridad de las oficinas, la empresa cuenta con un extintor por área y se pudo observar cámaras IP en el perímetro de la empresa. La oficina de oficina de almacén no cuenta con una cámara de seguridad en su interior, lugar donde se resguarda la mercadería de la empresa.

La seguridad en una red es un valor importante que todos los administradores deben de considerar, ya que de esta manera se garantiza máxima seguridad de los datos que viajan a través de la red de la empresa.

3.3.1.5. Controles para la instalación y uso de dispositivos externos.

Se pudo evidenciar que la empresa no cuenta con ninguna política de restricciones sobre el uso de dispositivos externos, todos los puertos USB de los ordenadores

no están bloqueados y estos permiten la conexión de dispositivos externos, si un trabajador tratara de utilizarlos, este no sería sancionado por la empresa.

El tener un control de las instalaciones de hardware y software evita que los trabajadores descontentos cometan fraude, robando información confidencial de la empresa o que instalen software innecesario para la misma.

3.3.2. Seguridad lógica.

3.3.2.1. Acceso de los usuarios a sistemas, sistemas operativos y base de datos.

En esta parte se pudo apreciar que más de la mitad de las computadoras del área comercial no cuenta con protección de acceso por contraseña, lo que supone un riesgo de seguridad debido a que cualquier persona puede iniciar sesión en el equipo e ingresar a la información almacenada en los discos duros

En cuanto al ingreso de los usuarios a sistemas, se pudo ver que el área comercial utiliza dos sistemas informáticos que requiere de un usuario y contraseña para el uso de los mismos. El primer sistema es el SEACE, el cual es un sistema del estado que permite que las empresas privadas puedan realizar ventas mediante licitaciones a entidades públicas. Este es un sistema web el cual requiere obligatoriamente de conexión a internet para su uso.

Del área comercial, de todos los empleados, solo cinco tienen acceso a este sistema. Si otra persona desea ingresar, uno de los empleados se dirige a la computadora del usuario, inicia sesión en el sistema y mantiene la sesión abierta durante el tiempo que el usuario haga uso de la aplicación

Debido a que el sistema no es de propiedad de la empresa, solo se pudo evaluar el resguardo de la contraseña de acceso, así como también el número de usuarios que lo usan y los trabajos que se realizan en él.

El segundo sistema empleado es el SoftLink, el cual es un software de gestión que abarca diferentes áreas de la empresa, como lo son de contabilidad, almacén y administración. Cada usuario tiene diferentes niveles de acceso de acuerdo a los privilegios otorgados por el administrador.

Los niveles de control en el acceso a los sistemas en una empresa son vitales, ya que aumentan los niveles de seguridad e integridad de la información, se baja enormemente los riesgos de fraude, filtración o alteración de la información, limitando en gran parte la cantidad de usuarios y administradores de los puntos críticos y manteniendo el control del flujo de la información.

3.3.2.2. Acceso de los usuarios a programas y archivos.

Para este punto se tuvo la información a través de observación y entrevistas, lo que se pudo notar que las políticas de la empresa establecen que los trabajadores que utilizan las computadoras solo deben de hacer el uso de los sistemas necesarios para el rubro de la empresa ya sea el SEACE o SoftLink, además del sistema operativo y el software de ofimática.

Esta prohibición es informada a los trabajadores de forma verbal, a través del encargado de administración y de recursos humanos.

Este registro es sumamente importante ya que la empresa desde el inicio deja claro a los trabajadores cuáles son sus obligaciones y responsabilidades en la empresa. Un mal uso por parte del empleado podría causar serios daños en los equipos, software y otros elementos relacionados con TI.

3.3.2.3. Disposición de sistemas alternos en caso de fallas.

Sobre la disposición de sistemas alternos, se pudo observar que la empresa no cuenta con tales sistemas. Tampoco se tiene un plan de contingencia en caso de

problemas. En caso que exista algún problema con los sistemas de gestión, se recurre al proveedor de internet a través de una llamada para generar un ticket

El uso de sistemas alternos es de vital importancia para la prevención de caídas de algún servicio por largos periodos de tiempo, si la empresa no cuenta con sistemas alterno para su funcionamiento, esto podría detener de manera parcial o total sus operaciones, lo que se vería reflejado en perdidas, los cuales pueden ocasionar cuantiosas pérdidas para la empresa.

3.3.2.4. Existencia de software de protección (antivirus y firewall).

Al verificar la presencia de algún software de protección, se pudo ver que no todas las computadoras cuentan con un sistema de protección estándar. Se pudo observar que no todos los equipos usan las mismas marcas de antivirus. El firewall en funcionamiento es el que viene integrado en el sistema operativo del equipo, el servidor no cuenta con un antivirus lo cual es un riesgo para el su sistema operativo.

La presencia de un software de protección actualizada es indispensable para la integridad y manejo de la empresa, al no contar con este tipo de seguridad hace que las computadoras de la empresa sean más vulnerables a cualquier ataque informático

3.3.2.5. Control de acceso de los usuarios a los servicios de internet.

Se puede observar que todos los equipos informáticos tienen conexión al servicio de internet y a la red de la empresa

El acceso a internet se restringe mediante un servidor con el sistema operativo Mikrotik. Este sistema permite configurar el límite de velocidad y

restringir el acceso a internet mediante el IP o la MAC de los dispositivos de red. La configuración la realiza el encargado de informática mediante indicaciones de gerencia de la empresa, quien es el que decide los permisos de acceso a internet por usuario, para lo cual se toma en cuenta el cargo y función de los empleados. Los jefes de cada área no tienen restricciones, mientras que los demás empleados si los tienen.

Tener el control de los accesos a internet reducen los riesgos que puedan afectar la integridad de la información, además certifica que la comunicación a través de dicho enlace sea utilizada para los objetivos y fines de la empresa.

3.3.4. Respaldos y planes de contingencia.

Al poder evaluar los módulos descrito en respaldos y planes de contingencia, se encontraron los siguientes hallazgos.

3.3.4.1. Respaldo de información crítica.

Para los respaldos de la información crítica se pudo encontrar que la empresa maneja un respaldo de información de sus clientes tanto de manera física como de manera digital y estos mismos están salva guardadas en las instalaciones de la empresa y un backup de esta información en el correo corporativo.

El respaldo de toda información crítica de la empresa es muy importante para la empresa, las empresas deben estar comprometidas con la cautela de su información para así poder asegurar que sus operaciones no sean afectadas por perdida de datos, contar con respaldos actualizados puede ser la solución en muchos casos de una recuperación rápida de las actividades comerciales.

3.3.4.2. Plan de continuidad.

En relación al plan de continuidad, la empresa no está preparada ante cualquier desastre natural si esto pasara, esta llegara a interrumpir sus acciones, no tienen contemplado que algo así pudiera interrumpir sus operaciones financieras, si existiera algún tipo de fallo en general la empresa quedaría deshabilitada, no existe un plan de continuidad

Un plan de continuidad es básico para poder mantener a la empresa operativa en el caso de ocurrir algún contratiempo de fuerza mayor.

3.3.4.3. Plan de contingencia.

En caso de pérdida de conexión a Internet, la empresa cuenta con un módem USB del ISP Claro para continuar con los accesos a los sistemas web. En el caso que el sistema SoftLink no esté disponible, la empresa cuenta con formatos que pueden ser llenados de forma manual.

Un plan de contingencia es muy trascendental ya que en el caso ocurriera algún tipo de falla la cual interrumpa parcialmente las actividades de la empresa, esta no quedaría fuera de operaciones. Con lo que no presentaría alguna perdida.

3.3.4.4. Plan de mantenimiento de hardware y software.

Se pudo notar que la empresa si cuenta con un programa para el mantenimiento de los equipos informáticos (hardware), este plan se pone en funcionamiento al inicio del año y a medio año. Para el caso de Software, este manteniendo se realiza solo cuando un programa o software presente inconveniente. Los mantenimientos son realizados por la oficina de soporte técnico de la empresa.

3.3.5. Documentación de hardware y software.

Al poder evaluar los módulos descritos en los documentos de hardware y software se pudo encontrar los siguientes hallazgos los que se describen a continuación.

3.3.5.1. Disposición de manuales de usuarios y de instalación de sistemas.

Se pudo evidenciar que para el caso del sistema SoftLink, sólo se tiene el manual de usuario. No se cuenta con el manual de instalación ni la documentación técnica, debido a que la adquisición del sistema aún no ha sido formalizada.

Para el caso de SEACE, se pudo observar que la documentación se encuentra en la página web del sistema.

Es muy importante para los usuarios, así como para el administrador de sistemas contar con documentación de los sistemas de información adquiridos por la empresa, ya que así es más fácil poder capacitar a los usuarios en el uso adecuado y eficiente del software, adema de poder saber cómo poder reinstalar el programa en caso que este sea necesario.

3.3.5.2. Existencia de documentación de adquisición de equipos y software y contratos legales del proveedor de internet.

Se pudo observar que la empresa si cuenta con la documentación necesaria y esta se encuentra resguardada por el área contable

Contar con este control es muy importante ya que de esta manera la empresa puede solicitar una garantía en el caso que algún equipo presente algún desperfecto en algún momento de ser requerido

3.3.5.3. Documentación técnica de los sistemas utilizados en la empresa.

Se pudo evidenciar que la empresa no cuenta con esta documentación, debido a que los sistemas utilizados han sido desarrollados por la empresa.

La falta de este tipo de documentación técnica de los sistemas dificulta el mantenimiento y la mejora de estos mismos.

3.3.6. Informe de hallazgos.

Se pudo definir que le informe de hallazgos dio evidencias del estado situacional de la empresa con respecto a sus sistemas de información, se han encontrado 20 hallazgos de acuerdo al plan de auditoría VER ANEXO (informe de auditoría)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Primera. Se ha cumplido con evaluar cada punto de los controles plasmados en el plan de auditoría, la auditoría revelo que los controles implementados no se han aplicado de forma adecuada, evaluando el área más importante de la empresa que es el área de comercial se pudo evidenciar la falta de manejo en el uso de las TICS.

Segunda. Se pudo evidenciar que la empresa OK Computer no tiene implementado de manera eficiente sistemas de control que le permitan tener el manejo de forma adecuada de sus sistemas.

Tercera. Se aplicaron técnicas de auditoría como son las de COBIT 4.1 el cual es un marco aceptado internacionalmente como una buena práctica para el control de la información de TI.

Cuarta. La auditoría informática es importante en la empresa para evaluar si las herramientas utilizadas sacan el máximo partido a la actividad empresarial esto se ve reflejado en el informe de hallazgos.

4.2 Recomendaciones

Primera. Se recomienda tomar en cuenta las recomendaciones planteadas en los diferentes hallazgos de la auditoría los cuales están debidamente documentados en este trabajo, recomendaciones que deben ser implementadas por el encargado de informática.

Segunda. Se recomienda programar cada cierto tiempo auditorías internas en el uso de TI para ver si la empresa sigue un horizonte informático y ver si se están implementado las recomendaciones de los trabajos de auditoría.

Tercera. Los hallazgos y observaciones de la auditoría informática deberán ser subsanados con las alternativas de solución recomendada o propia, de tal manera que aseguré el buen uso de las herramientas y la protección de la información de la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Alegsa, L. (2016). *Definición de software.* Recuperado de http://www.alegsa. com .ar /Dic/software.php

Alegsa, L. (2016). *Definición de UPS.* Recuperado de http://www.alegsa.com .ar/Dic/ups.php.

Álvarez, G., y Pérez, P. (2004). *Seguridad informática para empresas y particulares* (1ª ed.). España: McGraw-Hill.

Bembibre, V. (2017). *Definición de sistema*. Recuperado de https://www.defi nicionabc.com/general/sistema.php.

Castro, L. (2016). *¿Qué es ISP?* Recuperado de https://www. .aboutespanol.com/ que-es-isp-157852.

Concepto Definición. (2014). *Definición de Antivirus*. Recuperado de http://conceptodefinicion.de/antivirus/

Dordoigne, J. (2013). *Redes Informáticas. Nociones Fundamentales* (4ta ed.). España: Eni.

Fernández, S. (2015). *¿Qué es un Router y un módem? ¿En qué se diferencian?* Recuperado de http://www.valortop.com/blog/que-es-un-router-y-un-modem-en-que-se-diferencian

Gnome. (2017). *¿Qué es una dirección MAC?* Recuperado de https://help .gnome .org/users/gnome-help/stable/net-macaddress.html.es

Infortelecom. (2016). *Qué es un servidor y para qué sirve.* Recuperado de https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/

Joskowicz, J. (2013). *Cableado estructurado*. Recuperado de https://iie.fing. edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf.

Kaspersky. (s. f.). *¿Qué es un firewall?* https://www.kaspersky.es/resource-center/definitions/firewall.

Mikrotik Perú. (s. f.). *¿Qué es Mikrotik?* Recuperado de http://www.mikrotik peru.com/que-es-mikrotik.html.

Ramírez, G. (2009). *Sobre la auditoría informática y LOPD desde la experiencia personal y profesional.* Recuperado de https://e-archivo.uc3m.es /bitstream/handle/10016/6136/PFC_German_Ramirez_Rodriguez.pdf?se quence=1.

Stallings, W. (2004). *Comunicaciones y Redes de Computadores* (7ª ed.). México: Pearson.

TuElectrónica. (2017). *Qué es un cable de red UTP y sus mejoras*. Recuperado de https://tuelectronica.es/que-es-un-cable-de-red-utp-y-sus-mejoras/.

Vásquez, B. (2011). *Sistema operativo*. Recuperado de https://solvasquez. wordpress .com/2011/01/24/definición-de-sistema-operativo/.

Vialfa, C. (2017). *Intranet y extranet.* Recuperado de http://es.ccm.net /contents /213-intranet-y-extranet.

Wikipedia. (2017). *Copia de seguridad.* Recuperado de https://es.wikipedia. org/wiki/Copia_de_seguridad.

Wikipedia. (2017). *Correo electrónico*. Recuperado de https://es.wikipedia.org /wiki/Correo_electr%C3%B3nico.

Wikipedia. (2017). *Dirección IP.* Recuperado de https://es.wikipedia.org /wiki/ Direcci%C3%B3n_IP.

Wikipedia. (2017). *Hardware*. Recuperado de https://es.wikipedia.org /wiki /Hardware.

Wikipedia. (2017). *Unidad Rack*. Recuperado de https://es.wikipedia.org /wiki/Unidad_rack