UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

Evaluación de la seguridad y Eficiencia de los Sistemas Informáticos en una Empresa

AUTOR:

Bach. PORRAS AGAMA, CARLOS HUMBERTO

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

ASESOR:

Mg. HERMOZA OCHANTE RUBÉN EDGAR
ORCID: 0000-0003-2452-1524
DNI: 28237618

LIMA- PERÚ

2024

INFORME DE SIMILITUD

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

INFORME DE SIMILITUD

Nº022-2024-UPCI-FCI-REHO-T

A : **MG. HERMOZA OCHANTE RUBÉN EDGAR**
Decano (e) de la Facultad de Ciencias e Ingeniería

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional: **BACHILLER PORRAS AGAMA, CARLOS HUMBERTO**

FECHA : Lima, 1 de marzo de 2024.

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: **"EVALUACIÓN DE LA SEGURIDAD Y EFICIENCIA DE LOS SISTEMAS INFORMÁTICOS EN UNA EMPRESA"**, presentado por el Bachiller **PORRAS AGAMA, CARLOS HUMBERTO**.

2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 28%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).

3. Al término análisis, el Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

DEDICATORIA

A mis padres quienes me impulsan a ser mejor cada día y me ayudan a levantarme en cada caída.

AGRADECIMIENTO

Me gustaría agradecer a la Universidad por abrirme las puertas y brindarme la oportunidad de avanzar en mi carrera profesional.

INDICE

RESUMEN

OK Computer EIRL implementó una auditoría integral detallada que cubre aspectos informáticos, lógicos y físicos. COBIT se utiliza como marco de referencia durante este proceso. Durante el proceso de evaluación, se descubrieron una serie de problemas que amenazan la seguridad y que amenazan la integridad de la información de la empresa. Brindar recomendaciones para la eliminación de problemas descubiertos durante la inspección para asegurar el normal funcionamiento de la empresa. La importancia de la auditoría informática radica en la evaluación crítica de las herramientas utilizadas para garantizar que maximizan la eficiencia de las operaciones comerciales y garantizan la seguridad y protección de la información procesada

ABTRACT

OK Computer EIRL implemented a detailed comprehensive audit covering computer, logical and physical aspects. COBIT is used as a framework during this process. During the assessment process, a number of security-threatening issues were discovered that threaten the integrity of the company's information. Provide recommendations for the elimination of problems discovered during the inspection to ensure the normal operation of the company. The importance of computer audit lies in the critical evaluation of the tools used to ensure that they maximize the efficiency of business operations and guarantee the security and protection of the information processed.

CAPITULO I

INTRODUCCIÓN

OK Computer EIRL, especializada en tecnologías de la información, recomienda una auditoría exhaustiva que abarque tanto los aspectos lógicos como los físicos. La compañía está comprometida a brindar soluciones de extremo a extremo que incluyen software, hardware y servicios en diversas áreas como redes, telefonía, centros de datos, infraestructura, redes de acceso, soluciones inalámbricas, consultoría en desarrollo y ejecución de proyectos técnicos y licencias de software. y equipamiento técnico.

El objetivo es utilizar la auditoría informática como herramienta esencial para el análisis detallado de cada proceso empresarial. El objetivo principal es identificar las fortalezas y debilidades de la empresa en la gestión de estos procesos. Durante la ejecución de la auditoría se realiza una evaluación para determinar el grado de seguridad, planificación y eficiencia de los procesos en la organización.

A partir de los resultados de la auditoría se pretende mejorar los procesos que identifiquen debilidades en los sistemas y procedimientos de control, comunicación y empresa en las revisiones y evaluaciones. Al final de la auditoría informática, el objetivo es introducir recomendaciones para optimizar la eficiencia y seguridad de la información gestionada por la empresa y mejorar los métodos utilizados en la toma de decisiones.

CAPÍTULO II

OBJETIVO

2.1. Objetivo general

Desarrollar un plan de auditoría que aborde los elementos lógicos y físicos de los sistemas de información empresarial y la tecnología de comunicaciones de OK Computer EIRL.

2.2 Objetivos específicos

- Verifique que OK Computer Company tenga controles instalados.

- Implementar una metodología de auditoría informática diseñada para evaluar los controles frente a los riesgos informáticos.

-Preparar un informe sobre los hallazgos de la auditoría, incluidos los hallazgos y recomendaciones.

CAPÍTULO III

DESARROLLO DEL TEMA

Durante la auditoría de OK Computer EIRL Company se evaluará la gestión y eficiencia de la información, así como el curso de los procedimientos. Es muy importante el seguimiento continuo de la recopilación, procesamiento y almacenamiento de información respaldada por tecnología informática. En cualquier organización, el correcto desarrollo de estos procesos es fundamental para su óptimo funcionamiento.

Tras la finalización del análisis de auditoría, la Gestión Suprema podrá tomar decisiones destinadas a mejorar el uso de la infraestructura física y el sistema de información. Esto ayudará a optimizar el proceso de información y promover la mejora del servicio al cliente.

Además, al realizar esta auditoría, la empresa podrá identificar todos los riesgos relacionados con los procesos de TI y verificar la calidad y capacidad relacionadas con los requisitos de hardware y software.

3.1. Marco teórico

Primero se realizará una visión teórica de la auditoría para comprender aspectos como objetivos, definiciones, materialidad, diferencias, controles, riesgos, control interno, métodos, herramientas, funciones y planificación de la auditoría, y finalmente con un informe de auditoría en formato. de la presentación.

3.1.1. Generalidades de la auditoría

La función principal de una auditoría es brindar apoyo a la administración y su propósito es analizar y evaluar los controles internos de la empresa. Esto se hace considerando posibles acciones correctivas para garantizar la integridad de los activos, la precisión de la información y la eficacia continua de los sistemas de gestión.

La auditoría debe ser siempre independiente, no de carácter ejecutivo y sus conclusiones no vinculantes. La organización es libre de decidir sobre las acciones que queden pendientes tras su revisión.

El propósito de la auditoría es asegurar el uso correcto de la información en el entorno empresarial y la entrega oportuna de los resultados a la organización. Esto supone abarcar todas las evaluaciones relacionadas con las funciones, actividades y operaciones realizadas por los empleados y usuarios de la empresa.

El origen de la auditoría está relacionado con el importante crecimiento de la empresa, lo que generó la necesidad de realizar inspecciones para asegurar que los procesos de la organización se gestionen adecuadamente. El concepto actual de auditoría fue reconocido formalmente por primera vez en la Ley de Sociedades Británicas de 1862 y se formalizó durante el período legislativo correspondiente.

3.1.2.Tipos de auditoría.

La importancia de la auditoría para el funcionamiento eficaz de una organización ha creado la necesidad de una segmentación basada en áreas específicas que deben abordarse. Este enfoque tiene como objetivo mejorar el análisis cuando se inicia el proceso de auditoría.

3.1.2.1. Auditoría externa.

Este tipo de auditoría se realiza en colaboración con un equipo externo de profesionales para validar los estados financieros de la empresa. Este es un procedimiento utilizado con frecuencia para demostrar que una organización opera de manera transparente y ética.

3.1.2.2. Auditoría financiera

El objetivo principal es evaluar las cuentas de la organización a través del trabajo de un contador especializado en información contable. El objetivo es informar los resultados de este trabajo.

3.1.2.3. Auditoría fiscal

El propósito de este ejercicio es evaluar y obtener evidencia relacionada con hechos relevantes en materia tributaria.

3.1.2.4. Auditoría integral.

Este trabajo implica un análisis más crítico, exhaustivo y sistemático de los sistemas de información financiera, de gestión y legal de la organización. Esto se hace de forma autónoma utilizando métodos detallados para producir un informe completo que explica

la lógica detrás del estado de la información financiera. La evaluación se centra en la eficacia, eficiencia y economía de la gestión de recursos, así como en el cumplimiento de las operaciones financieras con las normas contables. El objetivo es tomar decisiones que aumenten la productividad de la empresa.

3.1.2.5. Auditoría interna de campo

Las auditorías in situ son responsabilidad de la dirección de la organización y están diseñadas para garantizar que se están cumpliendo los objetivos de la empresa.

3.1.2.6. Auditoría interna o auditoría contable financiera

La función principal de una auditoría es examinar y verificar la autenticidad de los informes y otros documentos administrativos y contables proporcionados por la dirección.

3.1.2.7.Auditoría informática

La auditoría informática es el resultado de recopilar, evaluar y clasificar evidencia para determinar si los sistemas de información protegen los activos de la empresa, mantienen la integridad de los datos, gestionan eficazmente los objetivos comerciales, administran eficazmente los recursos y cumplen con las leyes y regulaciones establecidas (Ramírez, 2009, p. 14).

El proceso de auditoría se centra en analizar los sistemas de control establecidos en la organización, comprobando su idoneidad y capacidad para alcanzar metas y estrategias predefinidas (Ramírez, 2009, p. 14).

3.1.3.COBIT 4.1

COBIT (Objetivos de Control de la Información y Tecnologías Relacionadas) es una referencia mundialmente reconocida como un conjunto de mejores prácticas para el control de la información y los riesgos relacionados con las tecnologías de la información (TI). COBIT se utiliza como herramienta para establecer el gobierno de TI y mejorar los controles relacionados con TI. Incluye objetivos de control, criterios de seguimiento, indicadores de desempeño, factores críticos y de éxito, y pautas de madurez.

COBIT significa Marco de Gestión de Tecnología de la Información (TI) y es a la vez un conjunto de herramientas y soporte para una gestión de TI eficaz. El marco proporciona a los gerentes una herramienta importante para cerrar la brecha entre los requisitos de control, los aspectos técnicos y los riesgos comerciales.

La implementación de COBIT ayuda a establecer políticas claras y buenas prácticas, mejorando así los controles de TI en toda la organización.

El marco enfatiza la importancia del cumplimiento, trabajando con las organizaciones para maximizar el valor de TI e impulsar la alineación mientras reduce la complejidad asociada con la implementación del marco COBIT.

3.1.3.1. Misión.

El principal objetivo de COBIT es desarrollar, investigar, promover y difundir un conjunto autorizado y actualizado de estándares internacionales. Estos estándares están diseñados para establecer prácticas comunes de gestión de TI y son ampliamente utilizados por gerentes y auditores en diversas organizaciones.

La función principal de COBIT es proporcionar orientación regulatoria internacional para los controles utilizados en entornos de tecnología de la información. El objetivo es garantizar que la organización alcance sus objetivos comerciales y confíe en el uso eficaz de la tecnología.

3.1.3.2 Estructura

COBIT ha integrado con éxito un enfoque que conecta el mundo de los negocios con el mundo de TI, reuniendo áreas que antes estaban distantes y requerían alineación.

La esencia de COBIT es el uso apropiado de los recursos de tecnología de la información (TI) a través de procesos de trabajo para satisfacer las necesidades de información de la organización.

3.1.3.4 Recursos de TI

COBIT se divide los recursos técnicos en diferentes categorías:

- **Datos:** Cobertura integral de todo tipo de información, incluida información interna y externa, estructurada y no estructurada, incluidos sonidos, gráficos y otros formatos.
- **Sistema de Información:** Incluye sistemas o aplicaciones que se operan mediante programación y programación manual.
- **Tecnología:** Incluye una amplia gama de elementos técnicos como sistemas operativos, hardware, software, equipos de telecomunicaciones, redes, vídeo, etc.
- **Instalaciones:** Se refiere a los recursos empresariales necesarios para soportar los sistemas de información.

- **Recursos humanos:** Incluye todas las habilidades y productividad de las personas que ayudan a adquirir, planificar, soportar y monitorear sistemas y servicios.

3.1.3.5 Proceso de Trabajo

Las áreas descritas en COBIT están organizadas según el modelo de ciclo de vida de gestión de recursos y constan de las siguientes categorías:

- Planificación y Organización (PO)
- Adquisición e Implementación (IA)
- Prestación de servicios y soporte (DS)
- Supervisión (hombres)

Estas áreas se dividen a su vez en subprocesos.

a. Planificación y Organización (PO).

P01 Desarrollar un plan estratégico del sistema.

P02 Desarrollar la arquitectura de la información.

P03 Conocer la dirección técnica.

P04 Determinar la dirección técnica.

P05 Gestionar las inversiones en TI.

P06 Comunicar metas y objetivos de gestión.

P07 Gestionar los recursos humanos.

P08 Velar por el cumplimiento de la normativa externa.

P09 Evaluar los riesgos.

P010 Proyecto de gestión

b. Adquisición e Implementación (A).

AI1. Adquirir y mantener software de aplicación.

AI2. Adquirir y mantener software de aplicación.

AI3. Aprender y mantener la arquitectura técnica.

AI4. Desarrollar y mantener procedimientos.

AI5. Implementar y validar sistemas de información

AI 6. Gestionar el cambio.

c. . Prestación de Servicios y Soporte (DS).

DS1. Crear niveles de servicio.

DS2. Servicios de administración.

DS3. Gestionar el rendimiento y la capacidad.

DS4. Garantizar la continuidad del servicio.

DS5. Garantizar la seguridad del sistema.

DS6. Determinar y asignar costos.

DS7. Educar y capacitar a los usuarios.

DS8. Proporcionar soporte y orientación a los clientes.

DS9. Administrar la configuración.

DS10. Resolver problemas e incidencias.

DS11. Información de gestión.

DS12. Gestionar locales.

DS13. Gestionar operaciones.

d. Monitoreo (M).

M1. Monitorear el proceso.

M2. Evaluar la eficacia del control interno.

M3. Obtenga una garantía independiente.

M4. Realizar una auditoría independiente.

3.1.3.6. Requerimientos del negocio.

Cuando se trata de COBIT, los requisitos comerciales se centran específicamente en los requisitos relacionados con la tecnología de la información.

a. Requerimientos de calidad.

- Calidad.
- Costos.
- Proporcionar servicios.

b. Requisitos de confianza.

- Eficiencia y eficacia operativa.
- Fiabilidad de la información.
- Cumplir con las leyes y reglamentos.

c. Requisitos de seguridad de la información.

- Confidencialidad.
- Honestidad.
- Disponibilidad.

3.2 Caso práctico

El proceso de auditoría se llevó a cabo en OK Computer EIRL utilizando el marco COBIT. El marco proporciona una serie de pasos como guía para realizar una evaluación. Las evaluaciones se realizaron en diferentes áreas de la empresa, identificando específicamente dónde se realizaban procesos informatizados.

3.2.1. Preliminar

OK Computer EIRL es una empresa especializada en la integración de tecnologías de la información. Inició sus operaciones el 22 de abril de 2004 y acumula más de 15 años de experiencia. Sus áreas de enfoque incluyen:

- Red
- Cooperación, telefonía, telemedicina.

- Centro de datos, virtualización de servidores.
- Infraestructura, cableado estructurado.
- Acceso a redes, fibra óptica y dispositivos externos
- Soluciones inalámbricas WAN y LAN
- Seguridad, videovigilancia, automatización.
- Proteccion eléctrica
- Soluciones interactivas
- Licencias de software
- Equipamiento técnico, impresión, materias primas.
- Leasing, subcontratación, arrendamiento financiero
- Consultoría y desarrollo de proyectos técnicos.

La organización cuenta con varios departamentos, incluidos los departamentos de contabilidad, proyectos, administración, almacén y comercial. Estas zonas están conectadas entre sí a través de la red interna propia de la empresa, lo que facilita el acceso a los servicios de red y permite la comunicación entre sí.

Veinticinco empleados utilizan los equipos informáticos de la empresa en las instalaciones. En este grupo se destacan los gerentes de soporte que son responsables de la administración tanto de hardware como de software.

El sector empresarial es el que más utiliza las tecnologías de la información. En este ámbito, los dos sistemas centrales que impulsan las actividades comerciales de la empresa son SEACE y SoftLink.

3.2.2. Justificación

Al realizar una auditoría en OK COMPUTER EIRL, el objetivo es evaluar cómo la empresa gestiona la información y qué métodos se utilizan. Por lo tanto, es necesario controlar cuidadosamente los procedimientos de recopilación, almacenamiento y procesamiento de información en una organización utilizando tecnología informática.

Con base en el análisis inicial de la empresa, se determinó que el foco de la auditoría serán las actividades comerciales.

3.2.2.2. Gestión de riesgos

La gestión de riesgos eficaz requiere que la alta dirección tenga una conciencia clara del riesgo, una comprensión profunda del apetito por el riesgo de la empresa, transparencia sobre los riesgos importantes y la integración de las responsabilidades de gestión de riesgos en las operaciones de la empresa.

3.2.2.2. Áreas a auditar

a. Seguridad Lógica

Verifique que existan políticas y procedimientos para proteger la información y los derechos de acceso de personas no autorizadas.

b. Seguridad Física

El objetivo es evaluar la integridad de la seguridad y la protección física de los datos, procedimientos, instalaciones, equipos de red y personal de la empresa.

c. Respaldo y plan de contingencia

La verificación de la existencia de copias de seguridad de la información esencial para el correcto funcionamiento de la empresa en formato digital o físico deberá cumplir con los requisitos pertinentes.

d. Documentación de hardware y software

Verificar la existencia de documentos relacionados con todas las compras informáticas de la empresa, como manuales, contratos y facturas. Además, debes comprobar si existe documentación que describa los sistemas que ha adquirido la empresa.

3.2.3. Adecuación.

Al realizar esta auditoría, se utilizaron diversas técnicas para recopilar datos y con la ayuda de estas técnicas se obtuvo la información necesaria para su posterior procesamiento. Las tecnologías utilizadas incluyen:

- Cuestionario: Conjunto de preguntas estructuradas diseñadas para obtener información de los encuestados.
- Entrevista: Actividad realizada por un auditor que proporciona un enfoque más técnico para recopilar información de las fuentes en comparación con respuestas más directas a las preguntas del cuestionario.
- Observación: El proceso de registrar visualmente detalles en un escenario real, registrando información en un formato adecuado para resolver un problema.

3.2.4. Guía de auditoría

3.2.5. Formalización.

La auditoría se formalizó en una reunión con la alta dirección de la empresa, donde se llegó a un acuerdo entre el responsable del día a día y el auditor. En esta reunión se determinan las áreas específicas de auditoría, las limitaciones, el alcance, la duración prevista del acceso y la evaluación.

3.3. Representación de resultados

3.3.1. Seguridad física.

Después de probar los componentes de seguridad física mencionados anteriormente, se llegaron a los siguientes hallazgos, como se describe a continuación.

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

Se señaló que el dispositivo puede ser utilizado por usuarios que trabajan en áreas administrativas.

Establecer controles de acceso a los dispositivos puede ayudar a prevenir la exposición de la información y los dispositivos, reduciendo así los riesgos relacionados con accidentes o actividad humana. Esto proporciona una mayor seguridad para la disponibilidad e integridad de la información.

3.3.1.2. Informe de acceso y visitas a las instalaciones

Se observó que la organización no mantenía un registro de control de acceso al edificio. La solicitud de ingreso al edificio se realiza de manera verbal, y al ingresar a las instalaciones no

se le pide identificación al visitante, simplemente se le pregunta cuál es el destino y qué está buscando. Aunque hay cámaras de seguridad grabando la visita.

El registro formal de los visitantes de la empresa y de los empleados externos es esencial ya que ayudará a crear un entorno seguro para los empleados internos. Además, esta medida protege los activos, asegura la continuidad del negocio y protege los derechos de propiedad intelectual de la empresa.

3.3.1.3. Inventario de equipos y software

Respecto al inventario de los equipos y software de la empresa, se encontró que la empresa cuenta con un sistema de almacenamiento de equipos informáticos y electrónicos, tanto operativos como no operativos. Existe un registro manual que registra información sobre el dispositivo y su estado operativo. El software SoftLink incluye un módulo de contabilidad que los gerentes de logística utilizan para realizar un seguimiento del inventario de equipos de la empresa.

Las empresas necesitan un inventario de hardware y software actualizado para controlar directamente todos sus activos de tecnología de la información. Esto proporciona una comprensión precisa de los recursos almacenados y facilita la toma de decisiones sobre nuevas compras si es necesario.

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

La infraestructura de red de la empresa se compone principalmente de cables planos. El Proveedor de Servicios de Internet (ISP) (en este caso Movistar) brinda un servicio de doble núcleo que brinda acceso a Internet a una velocidad de 8 Mbps. Esta conexión se utiliza para un enrutador proporcionado por el ISP ubicado en una oficina de almacén y almacenado en un

gabinete cerrado con llave de 24 bastidores. Además, cuentan con un UPS como energía de respaldo que puede funcionar de manera continua durante 2 horas.

La infraestructura de red de la empresa se divide en cuatro subredes diferentes, a saber:

- Telefonía
- Administración
- Sección Comercial
- Proyectos

En una red, los cables UTP corren a lo largo de cables hasta llegar al dispositivo y conectarse directamente al puerto de red de la computadora. No hay paneles para ningún punto de datos. Está claro que el único estándar de cableado estructurado que se sigue durante la transmisión de datos es EIA/TIA. Además, la empresa cuenta con un sistema inalámbrico que brinda respaldo a algunos empleados utilizando puntos de acceso ubicados en las áreas de ventas y administrativas. Ambos dispositivos implementan medidas de seguridad como el filtrado por dirección MAC y claves WPA.

En cuanto a la seguridad de la oficina, es importante resaltar que la empresa cuenta con extintores para cada zona y se observó que se instalaron cámaras web alrededor de la oficina. Sin embargo, la oficina del almacén no cuenta con cámaras de seguridad internas, aunque la sala protegería la mercancía de la empresa.

La ciberseguridad es un valor clave que todo administrador debe considerar, ya que garantiza la máxima protección de los datos que fluyen por la infraestructura de la empresa.

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

Se observó que la empresa carecía de políticas que restringieran el uso de dispositivos externos; Se desbloquearon todos los puertos USB de las computadoras, lo que permitió conectar dispositivos externos sin penalización para los empleados que intentaran usarlos.

Implementar controles de instalación de hardware y software es fundamental para evitar que los empleados descontentos participen en actividades fraudulentas, como robar información confidencial de la empresa o instalar software no autorizado.

3.3.2. Seguridad lógica.

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

En este apartado, encontramos que más del 50% de los ordenadores empresariales carecen de protección con contraseña. Este es un riesgo para la seguridad porque cualquiera puede iniciar sesión en estas computadoras y acceder a la información almacenada en el disco duro.

Con respecto a los sistemas de acceso de usuarios, se observó que en el distrito comercial se utilizaban dos sistemas informáticos que requerían nombres de usuario y contraseñas. El primer sistema es SEACE, una plataforma gubernamental que permite a las empresas privadas vender a las autoridades públicas mediante licitaciones. El sistema funciona a través de Internet y requiere una conexión a Internet para funcionar.

En las empresas, sólo cinco de todos los empleados tienen acceso al sistema. Si otra persona quiere iniciar sesión, uno de los empleados se acerca a la computadora del usuario, inicia sesión en el sistema y permanece conectado mientras el usuario usa la aplicación.

Dado que el sistema no es propiedad de la empresa, esta solo puede evaluar la seguridad de las contraseñas y determinar la cantidad de usuarios que utilizan el sistema y las funciones que realizan dentro del mismo.

El otro sistema utilizado es SoftLink, un software de gestión que cubre diversas áreas del negocio como contabilidad, almacenamiento y administración. A cada usuario se le otorga un nivel de acceso diferente según los permisos brindados por el mismo administrador.

La implementación de una jerarquía de control de acceso al sistema en la empresa es fundamental porque ayuda a incrementar el nivel de seguridad e integridad de la información. Este enfoque reduce en gran medida los riesgos de fraude, fuga o alteración de datos al limitar significativamente la cantidad de usuarios y administradores que tienen acceso a puntos clave, manteniendo al mismo tiempo un estricto control sobre el flujo de información.

3.3.2.2. Acceso de usuarios a programas y archivos

Se realizaron observaciones y entrevistas para recopilar esta información. La investigación encontró que la política de la empresa dictaba que los empleados que utilizaban computadoras sólo debían utilizar los sistemas necesarios para los departamentos de la empresa, como SEACE o SoftLink, además de los sistemas operativos y el software de oficina.

Esta restricción se comunica verbalmente a los empleados a través de recursos administrativos y humanos.

Estos registros son importantes porque la empresa informa claramente a los empleados desde el inicio de sus deberes y responsabilidades en la organización. El uso inadecuado por parte de los empleados puede causar daños importantes a los equipos, software y otros elementos relacionados con TI.

3.3.2.3.Disposicion de sistemas alternos en caso de fallas.

Respecto a la disponibilidad de sistemas alternativos, se observó que la empresa no cuenta con dichos sistemas. Además, no tiene ningún plan de contingencia en caso de que algo salga mal. Si hay un problema con el sistema de control, la empresa genera un ticket llamando al proveedor de servicios de red para pedir ayuda.

La implementación de sistemas alternativos es fundamental para evitar interrupciones prolongadas del servicio. La falta de estos sistemas puede detener total o parcialmente el funcionamiento de la empresa y provocar pérdidas importantes a la organización.

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

Al comprobar la presencia de software de protección, notamos que no todos los ordenadores están equipados con sistemas de protección estándar. Vale la pena señalar que no todas las computadoras usan la misma marca de software antivirus y los firewalls que funcionan son los integrados en el sistema operativo de cada computadora. Además, se descubrió que el servidor carecía de software antivirus, lo que suponía un riesgo para su sistema operativo.

Tener un software de seguridad actualizado es esencial para garantizar la integridad y seguridad de su negocio. La falta de tales medidas de seguridad hace que las computadoras de la organización sean más vulnerables a posibles ataques informáticos.

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

Se observó que todos los equipos de cómputo se encontraban conectados a los servicios de Internet y a la intranet de la empresa.

Restrinja el acceso a la red utilizando servidores que ejecuten el sistema operativo Mikrotik. Este sistema le permite establecer límites de velocidad y restringir el acceso a Internet utilizando la dirección IP o la dirección MAC de su dispositivo de red.

La configuración de este sistema la realizan los responsables de TI bajo la dirección de la dirección de la empresa. La gerencia determina los derechos de acceso a la red de cada usuario en función del puesto y las funciones del empleado. El responsable de cada región no tiene restricciones, pero el resto de empleados sí las tienen.

El control de acceso a la red ayuda a reducir los riesgos que pueden afectar la integridad de la información. Además, garantiza que la comunicación a través de este enlace se utilice para las metas y objetivos declarados de la empresa.

3.3.4. Respaldos y planes de contingencia

Una evaluación de las modificaciones relacionadas con el despido y la planificación de contingencias reveló los siguientes hallazgos.

3.3.4.1. Respaldo de información crítica

En cuanto al respaldo de información crítica, se observó que la empresa realiza respaldos físicos y digitales de la información de los clientes. Estas copias de seguridad se guardan en las instalaciones de la empresa y también se realiza una copia de seguridad de esta información en el correo electrónico de la empresa.

Realizar una copia de seguridad de toda la información más importante de la empresa es fundamental, ya que garantiza la preservación de los datos y asegura la continuidad del negocio en caso de una posible pérdida. Mantener sus copias de seguridad actualizadas es fundamental para reanudar rápidamente el negocio en caso de circunstancias imprevistas.

3.3.4.2. Plan de continuidad.

En términos de planificación de continuidad, la empresa aún no ha implementado medidas de emergencia en caso de desastres naturales que puedan alterar las operaciones de la empresa. La falta de planificación de contingencias significó que la empresa no consideró la posibilidad de que eventos imprevistos afectaran su desempeño financiero, haciéndola inviable en caso de quiebra total.

Desarrollar un plan de continuidad del negocio es esencial para garantizar la continuidad del negocio en caso de imprevistos importantes.

3.3.4.3. Plan de contingencia.

En caso de una interrupción de la red, la Compañía podrá utilizar un módem USB proporcionado por Claro ISP para mantener el acceso a los sistemas de la red. Si el sistema SoftLink no está disponible, las empresas pueden completar el formulario manualmente.

La implementación de planes de emergencia es fundamental porque en caso de una interrupción que interrumpa parcialmente el negocio, el negocio continuará operando y evitará pérdidas.

3.3.4.4. Plan de mantenimiento de hardware y software.

Se observó que la empresa implementó un plan de mantenimiento de equipos de cómputo (hardware) el cual se realizó a inicios y mediados de año. El software solo recibe servicio si hay un problema con el programa o el software. La oficina de soporte técnico de la empresa se encarga de estas tareas de mantenimiento.

3.3.5. Documentación de hardware y software

La evaluación de los módulos relacionados con la documentación de hardware y software identificó los siguientes resultados, los cuales se detallan a continuación.

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

En el caso del sistema SoftLink se observó que solo se entregó el manual de usuario, faltando el manual de instalación y la documentación técnica ya que aún no se había concretado la compra del sistema. En cuanto a SEACE, encontré que hay documentos relevantes en el sitio web del sistema.

La documentación completa del sistema de información es esencial tanto para los usuarios como para los administradores del sistema, ya que ayuda en la capacitación de los usuarios y garantiza una reinstalación eficiente del software cuando sea necesario.

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

La empresa cuenta con los documentos necesarios que se almacenan en el área de contabilidad.

Mantener este control es muy importante porque permite a la empresa reclamar la garantía si algún equipo presenta algún defecto en cualquier momento.

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

La empresa no dispone de esta documentación porque el sistema utilizado es de desarrollo propio.

La falta de documentación técnica para el sistema puede complicar el mantenimiento y las actualizaciones.

3.3.6. Informe de hallazgos.

Se encontró que la revisión de desempeño proporcionó evidencia del estado actual de los sistemas de información de la empresa y se identificaron un total de 20 hallazgos de acuerdo con el plan de auditoría.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. La auditoría del sistema informático de OK Computer EIRL reveló que el sistema en uso carecía de documentación técnica, dificultaba su mantenimiento y mejoras. Esta deficiencia puede comprometer la eficiencia y seguridad de la información gestionada por la empresa.

2. El uso de técnicas de auditoría computarizadas permite la identificación de hallazgos importantes y su detalle en el informe de auditoría. Estos resultados proporcionan una indicación clara del estado de la empresa en relación a sus sistemas de información.

3. La auditoría realizada proporcionó a la alta dirección de OK Computer EIRL la información necesaria para tomar decisiones encaminadas a mejorar el funcionamiento de la red y el uso de los sistemas de información de su unidad estructural12. Esto demuestra el valor de la auditoría como herramienta de toma de decisiones estratégicas en la industria de TI.

4. El estudio destaca la importancia de las auditorías lógicas y físicas de los sistemas de información y tecnologías de comunicación de la empresa para garantizar la eficiencia, seguridad y calidad de la gestión de la información e identificar posibles riesgos informáticos.

4.2. Recomendaciones

1. Crear y mantener documentación técnica completa de los sistemas informáticos utilizados por OK Computer EIRL. Este documento debe incluir información detallada sobre infraestructura, configuración, procedimientos de mantenimiento y cualquier otra información relevante que ayude a gestionar el sistema de forma eficaz.

2. Implementar las recomendaciones del informe de auditoría para abordar los problemas identificados.

3. Priorizar y ejecutar estas acciones correctivas de manera oportuna es fundamental para reducir el riesgo y mejorar la eficiencia y seguridad de los sistemas de información de una empresa.

4. Crear un proceso continuo de auditoría y seguimiento de los sistemas informáticos de la empresa. Esto garantizará que la gestión de la información mantenga un alto nivel de seguridad, eficiencia y calidad y que los riesgos potenciales de TI se identifiquen de manera oportuna. Haga de la auditoría informática una parte importante de las decisiones estratégicas de su empresa. Esto incluye el uso de resultados de auditoría para respaldar la planificación y asignación de recursos para mejorar el rendimiento de la red física y el uso de sistemas de información para optimizar el servicio al cliente y mejorar la competitividad de la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Alegsa, L. (2016). Definición de software. Recuperado de http://www.alegsa. Com

.ar /Dic/software.phpAlegsa, 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.definicionabc.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 dehttps://archivo.uc3m.e/bitstream/handle/10016/6136/PFC_German_Ramirez_Rodrigz.pdf?s e 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.

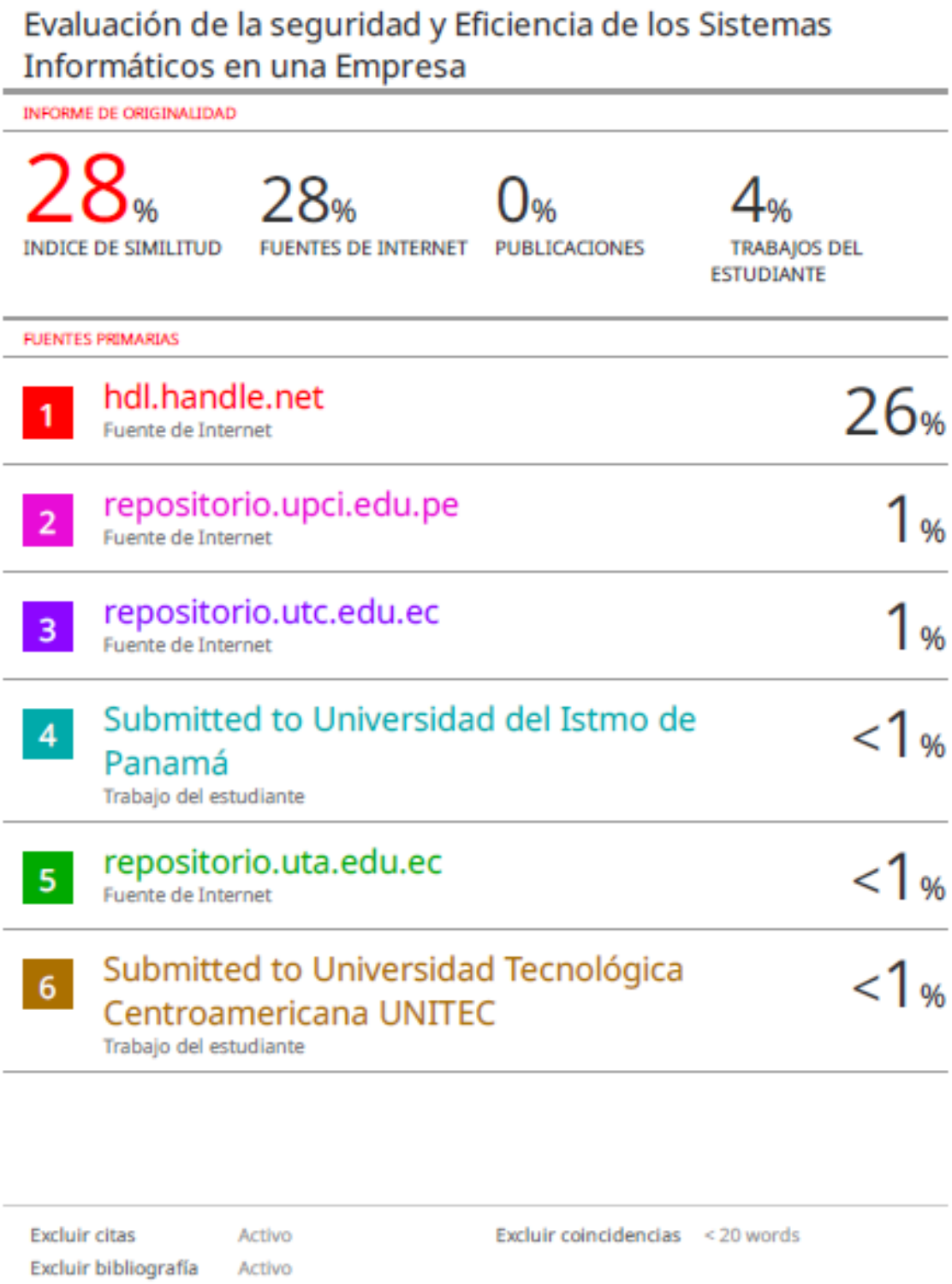
Wikipedia. (2017). Correo electrónico. Recuperado de https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico.

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). UnidadRack. Recuperado de https://es.wikipedia.org /wiki/Unidad_rack

ANEXOS

Anexo 1. Evidencia de similitud digital



Evaluación de la seguridad y Eficiencia de los Sistemas Informáticos en una Empresa

INFORME DE ORIGINALIDAD

28%	28%	0%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	26%
2	repositorio.upci.edu.pe Fuente de Internet	1%
3	repositorio.utc.edu.ec Fuente de Internet	1%
4	Submitted to Universidad del Istmo de Panamá Trabajo del estudiante	<1%
5	repositorio.uta.edu.ec Fuente de Internet	<1%
6	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1%

Excluir citas	Activo	Excluir coincidencias	< 20 words
Excluir bibliografía	Activo		

Anexo 2: Autorización de publicación en repositorio

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACION O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: PORRAS AGAMA CARLOS HUMBERTO

DNI: 70124449 Correo electrónico: carlinhpa@gmail.com

Domicilio: JR AYACUCHO Nº 1041

Teléfono fijo: _____ Teléfono celular: 999578709

2.- IDENTIFICACIÓN DEL TRABAJO o TESIS

Facultad/Escuela: INGENIERIA DE SISTEMAS E INFORMÁTICA.

Tipo: Trabajo de Investigación Bachiller ( ) Tesis ( ) Trabajo de Suficiencia Profesional (X)

Título del Trabajo de Investigación / Tesis:

EVALUACIÓN DE LA SEGURIDAD Y EFICIENCIA DE LOS SISTEMAS INFORMÁTICOS EN UNA EMPRESA

3.- OBTENER:

Bachiller ( ) Titulo (X) Mg ( ) Dr ( ) PhD ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRONICA

Por la presente declaro que el (trabajo/tesis) trabajo indicada en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencia e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art 23 y Art. 33.

Autorizo la publicación (marque con una X):
(X) Sí, autorizo el depósito total.
( ) Sí, autorizo el depósito y solo las partes: _____
( ) No autorizo el depósito.

Como constancia firmo el presente documento en la ciudad de Lima, a los ____ días del mes de _____ de _____.

Huella digital

Firma