

Universidad Técnica Nacional

Sede Regional de San Carlos

Ingeniería del Software



Informe final proyecto de Auditoría de Sistemas

Docente:

Freddy Gerardo Rocha Boza.

Elaborado por:

Andrey Carranza Pérez

Jorge Vinicio Araya Torres

Jose Pablo Bolaños Calvo

Gerardo Espinoza Vargas

Ciudad Quesada, Agosto 2021

Contenido

Auditoria Informática.....	3
Resumen Ejecutivo.....	4
Introducción	5
Alcance.....	6
Objetivos.....	6
Objetivo General	6
Objetivos Específicos	6
Metodología.....	6
Planificación	7
Carta solicitud de Auditoría:	8
Carta de Introducción Informe Final de la Auditoria	8
Hallazgos.....	9
Estructura Organizacional Recursos Humanos	10
Seguridad de la información	12
Revisión de Software	17
Seguridad Física	20
Conclusiones	24
Bibliografía.....	25

Auditoria Informática

El proceso sistemático por el cual un equipo o una persona competente e independiente obtiene y evalúa objetivamente la evidencia respecto a las afirmaciones acerca de un proceso con el fin de formarse una opinión sobre el particular e informar sobre el grado de cumplimiento en dicha afirmación es implementada.

Tipos más comunes de Auditoria Informática:

- Auditoría Interna.
- Auditoría Externa.
- Auditoría Financiera.
- Auditoría Integrada.
- Auditoría Operativa.
- Auditoría de Tecnología.
- Auditoría de TI.
- Auditoría Continua.
- Auditoría Forense.

Los principales objetivos que constituyen a la auditoria Informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

Resumen Ejecutivo

El presente trabajo tiene como objetivo determinar cuáles son los diferentes procesos que el Hotel el descanso en la montaña maneja en su día a día, así como identificar cuáles de estos se están realizando correctamente y cuáles no, mediante los procesos que conlleva realizar una auditoría, mediante el análisis de procesos y documentación. Al momento de analizar o estudiar un proceso se redactará un papel de trabajo en el cual se mencionará cual es la función para analizar, se identificará si existe algún tipo de evidencia y que preguntas se le realizan al momento de entrevistar al encargado de dicha área, posteriormente para cada papel de trabajo se redactará una conclusión la cual será la base para construir el hallazgo. Toda esta información debe ser comunicada hacia todos los funcionarios de la entidad, o personas interesadas, para que ellos puedan evaluar de forma independiente los sistemas de la organización.

El realizar un proceso de auditoria completo nos indica que se deben analizar las diferentes áreas de cualquier empresa, en este caso el Hotel el descanso en la montaña, posee una serie de departamentos, como recursos humanos, tecnología de la información, seguridad física y demás, cada área de estas debe de contar con sus respectivas políticas, colaboradores, manuales de puestos, gerencias etc., mencionamos esto ya que el análisis de procesos de realizaría de manera individual por cada uno de estos departamentos así que los papeles de trabajo y los hallazgos, nunca se tendrían que mezclar.

Introducción

Actualmente para garantizar el éxito de cualquier empresa, se deben de tener una estructura sólida, en donde los procesos deben de estar claros y bien definidos, debido a esto se realizan las auditorías lo cual nos permite realizar un chequeo, ya sea general, o por sesiones de cómo está la empresa, identificando muchos factores, como: procesos mal realizados, falta de documentación, falta de políticas, capacidades del personal u otras. Es importante saber que existen muchos tipos de auditorías según el área, por ejemplo: Auditoría financiera, administrativa, operacional, integral, de sistemas etc. Y que estas pueden darse en diferentes orígenes, ya sea, externa o interna.

Para garantizar el éxito de una empresa no solo se debe considerar si un proceso se está realizando de la mejor manera, sino que implica otros factores como el saber si mis colaboradores están bien capacitados, si están desempeñando una función según su profesión, toda esta información puede ser muy difícil determinarla sin un proceso determinado, gracias a la auditoría se puede determinar con un gran porcentaje de exactitud qué cosas se están realizando bien y cuáles no, una de las grandes ventajas es que estos estudios los realizan personas capacitadas, que tienen un criterio y visión muy amplia, el cual nos puede guiar con mejoras muy importantes que nos puede garantizar grandes ganancias económicas a corto y largo plazo, ya que se podrá tener una evolución global y objetiva de la entidad las cuales serían interpretadas de manera parcial por los departamentos afectados, además de que se pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa y favorece a la protección de los intereses y bienes de la empresa frente a terceros.

Es importante el tener una noción a grandes rasgos de cuáles son los procesos que conlleva a realizar un proceso de este tipo, tanto desde el punto de vista de un auditor como de un empleado, por lo que en este proyecto se va a enfocar en poder estudiar ambas partes sin afectar el objetivo principal el cual será ayudar a la dirección general a evaluar de forma relativamente independiente los sistemas de la organización de administración. Este trabajo tendrá dos partes muy importantes la primera será la de los papeles de trabajo, la cual será la plantilla para registrar los datos que el auditor recolecta por cada proceso, la segunda será la de los hallazgos, la cual consiste en determinar cuáles son las debilidades en el control interno, detectadas por el auditor.

Alcance

La auditoría se realizará sobre las diferentes áreas, en su estructura, administración de recursos humanos, software y seguridad física del departamento de TI del hotel descanso en la montaña.

Objetivos

Objetivo General

- Definir y evaluar el estado general de la empresa Hotel descanso en la montaña en su estructura, administración de recursos humanos, software y seguridad física.

Objetivos Específicos

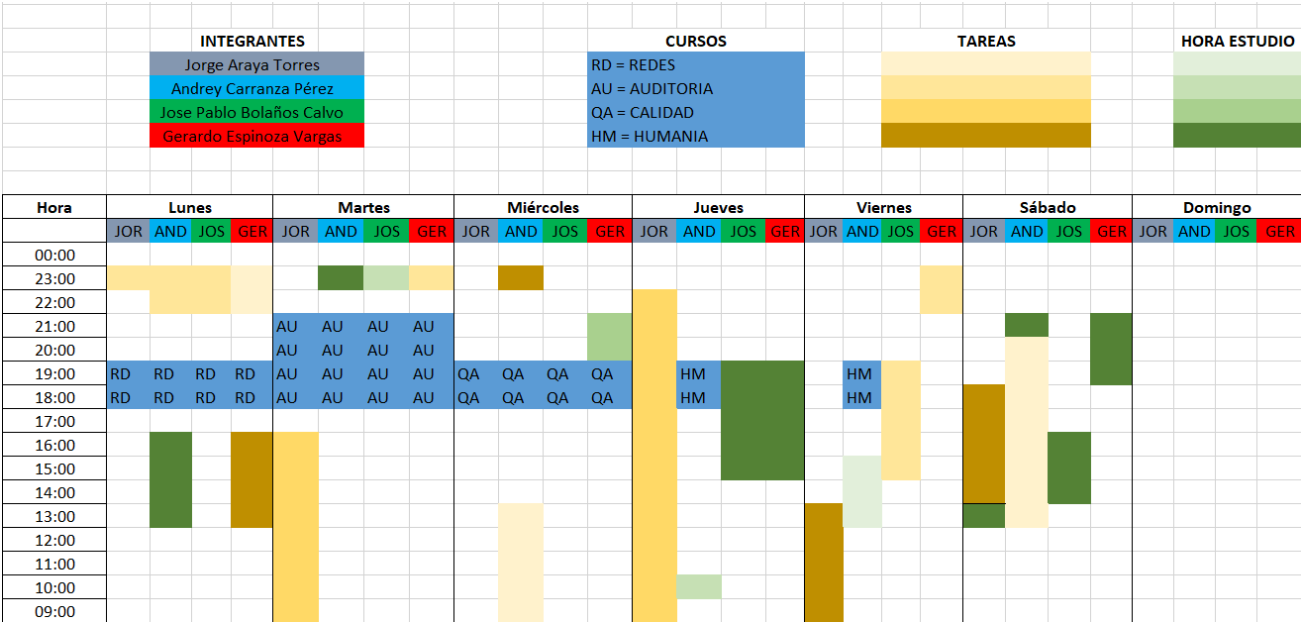
- Verificar que se cumpla con las políticas internas, así como los criterios de Optimizar la ubicación de la función de TI (COBIT 5) en la empresa.
- Identificar los puntos de mejora en las diferentes áreas (estructura, administración de recursos humanos, software y seguridad física en TI).
- Conocer las posibles causas que estén atentando contra las buenas prácticas y políticas de la empresa en el área de TI.

Metodología

La elaboración de esta auditoria tenía como finalidad evaluar cada objetivo como los inconvenientes que se pudieran presentar en el desarrollo de esta. La evaluación respectiva que se realizó a la empresa Hotel el descanso en la montaña se trató de emplear los métodos de recopilación de datos, como una serie de actividades que nos ayudaron a realizar la auditoria. Los papeles de trabajo cumplen con la finalidad de guardar pruebas de nuestro trabajo realizado como medio de demostrar, cualquier momento la amplitud y la evidencia de los hechos y poder expresar los procedimientos de auditoria utilizados. Además de la implementación de apoyo por medio de técnicas especiales de auditoria para la evaluación de los sistemas computaciones como el comportamiento de los sistemas que están siendo auditados. La evaluación de los sistemas computaciones como el área de sistemas computaciones la importancia de evaluar cada aspecto como el acceso, uso, mantenimiento y resguardo de las bases de datos. La evaluación administrativa evaluar aspectos como la misión, visión, objetivos, estrategia, planes, programas, estructura de organización, perfil de puestos. La evaluación de la documentación se necesitó evaluar aspectos como la seguridad

y la protección de los archivos informáticos, instalaciones. Evaluación del desarrollo de proyectos informáticos, estandarización de metodologías, programas, equipos, sistemas, mobiliario. Lista de verificación (o lista de chequeo). Instrumento que contiene criterios o indicadores a partir de los cuales se miden y evalúan las características del objeto, comprobando si cumple con los atributos establecidos. La lista de verificación se utiliza básicamente en la práctica de la investigación que forma parte del proceso de evaluación.

Planificación



Fuente: Autoría Propia

Carta solicitud de Auditoría:

Carta de Introducción Informe Final de la Auditoria

Hotel descanso en la montaña
Ciudad Quesada, 31 de Julio de
2021

Estimados

Hotel descanso en la montaña
Atte. Sr. Freddy Rocha Boza

De nuestra consideración:

Tenemos el agrado de dirigirnos a Ud. a efectos de elevar a vuestra consideración el alcance del trabajo de Auditoría del Área de Informática practicada los días entre el 10 de mayo al 03 de agosto de 2021, del corriente, sobre la base del análisis y procedimientos detallados de todas las informaciones recopiladas y emitidos en el presente informe, que a nuestro criterio es razonable.

Síntesis de la revisión realizada, clasificado en las siguientes secciones:

A. Organización y Administración del Área

B. Seguridad física y lógica

C. Desarrollo y mantenimiento de los sistemas de aplicaciones.

El contenido del informe ha sido dividido de la siguiente forma a efectos de facilitar su análisis.

a. Situación. Describe brevemente las debilidades resultantes de nuestro análisis.

b. Efectos y/o implicancias probables. Enuncian los posibles riesgos a que se encuentran expuestos las operaciones realizadas por la Cooperativa.

c. Índice de importancia establecida. Indica con una calificación del 0 al 3 el grado crítico del problema y la oportunidad en que se deben tomar las acciones correctivas del caso.

Atentamente.

Gerardo E.V

Andrey C.P

Jorge A.T

Pablo B.C

Hallazgos

Hotel descanso en la montaña

Fecha de redacción del informe:
Ciudad Quesada, 31 de Julio de
2021

Identificación del informe
Auditoría Interna

Identificación del Cliente
Freddy Gerardo Rocha Boza

Identificación de la Entidad Auditada
Hotel descanso en la montaña

Fecha de Ejecución
10/05/2021 – 03/08/2021


Equipo auditor:


Andrey Carranza Pérez,
Gerardo Espinoza Vargas,
Jose Pablo Bolaños Calvo,
Jorge Araya Torres


Personas entrevistadas:


Freddy Gerardo Rocha Boza


Estructura Organizacional Recursos Humanos


Solicitud de la reseña de la empresa		
1. Cumple con el requerimiento establecido		
Observación de la Administración		
Existe la reseña de la organización, junto a sus antecedentes, misión, visión, y un organigrama con los departamentos y responsables.		
Aceptación		
Si 	No	Parcial


Solicitud de Organigrama Organizacional		
2. Cumple con el requerimiento establecido		
Observación de la Administración		
El departamento de tecnología es directamente proporcional a la importancia de esta unidad, y se comprueba un nivel suficiente de independencia.		
Aceptación		
Si 	No	Parcial


Solicitud de Organigrama de T. I		
3. Cumple con el requerimiento establecido		
Observación de la Administración		
Hay conformidad, ya que existe un organigrama de esta entidad.		
Aceptación		
Si 	No	Parcial


Solicitud de lista del personal de T. I		
4. Cumple con el requerimiento establecido		
Observación de la Administración		
Hay conformidad, ya que existe un documento con la lista del personal de esta área.		
Aceptación		
Si 	No	Parcial


Solicitud de lista de perfiles de puesto de T. I		
5. No cumple con los requerimientos establecidos		
Incumple APO07.02, identificar personal clave de TI		
Observación de la Administración		
No hay conformidad, ya que existen discrepancias entre la lista de personal y el documento de perfiles de puestos en la empresa, solamente el analista de sistemas Jesus Torres Cruz cumple con los requerimientos. Además, no existe una lista con los suplentes donde se compruebe su existencia.		
Aceptación		
Si	No 	Parcial
Recomendación: Presentar una lista adecuada y correcta del personal del área de TI		

Vacaciones acumuladas
6. No cumple con los requerimientos establecidos
Incumple APO07.06 gestionar personal contratado
Observación de la Administración
No hay conformidad, ya que no existen documentos para analizar este aspecto.
Aceptación
Si No  Parcial
Recomendaciones: Poseer un documento de control de vacaciones acumulados por miembro.


Entrevista de funcionarios en cada unidad
7. No cumple con los requerimientos establecidos
Incumple la política APO07.04 evaluar el desempeño laboral de los empleados.
Observación de la Administración
No se encuentra ningún documento que corrobore su existencia.
Aceptación
Si No  Parcial
Recomendaciones: Implementar políticas para llevar a cabo evaluaciones de rendimiento del personal.

Vacaciones acumuladas por género
8. No cumple con los requerimientos establecidos
Incumple APO07.06 gestionar personal contratado
Observación de la Administración
No existen pruebas para realizar el análisis.
Aceptación
Si No  Parcial
Recomendaciones: Poseer un documento de control de vacaciones acumulados por género.

Perfil del departamento de gerencia de TI
9. Si cumple con los requerimientos establecidos
Observación de la Administración
Existe un documento con los perfiles de gerencia de TI.
Aceptación
Si  No Parcial

Solicitar copia del contrato
10. Si cumple con los requerimientos.
Observación de la Administración
Se dispone de las respectivas copias de las plantillas de contrato del Hotel el Descanso.
Aceptación
Si  No Parcial


Hallazgos positivos


Plantilla de contrato		
11. Si cumple con los requerimientos.		
Observación de la Administración		
Se presenta una plantilla de contrato muy bien definida y que cumple con los requerimientos empresariales.		
Aceptación		
Si		No Parcial

Conclusiones papel de trabajo:


En general, el área de recursos humanos la mayor parte de los hallazgos encontrados fueron conformes con un 64%, y la no conformidad con un 36% es importante que los hallazgos que presentan no conformidad sean corregidos para la mejora de puntos importantes de recursos humanos, como por ejemplo los perfiles de puestos de TI, ni el documento de vacaciones acumuladas, rendimiento de los empleados, y tampoco existe un documento de vacaciones acumuladas por género.


Seguridad de la información


Verificar la existencia de mecanismos utilizados para la encriptación de información sensible		
1. Cumple con el requerimiento establecido		
Observación de la Administración		
Existe una norma que respalda el proceso de encriptación de información sensible, de igual forma se puede evidenciar este proceso de encriptación en los dispositivos de almacenamiento externo.		
Aceptación		
Si		No Parcial


Verificar la utilización de perfiles de VPN para cada uno de los empleados del área de tecnologías de información		
2. Cumple parcialmente con el requerimiento establecido		
Observación de la Administración		
Se realiza una asignación de ip que se guarda para cada máquina de las respectivas áreas de la empresa, pero no existe evidencia de la utilización de alguna VPN.		
Aceptación		
Si	No	Parcial 


Verificar que los empleados ingresen a las reuniones desde su respectivo correo empresarial.		
3. Cumple con el requerimiento establecido		
Observación de la Administración		
Se evidencia el uso de correos empresariales para estas reuniones y procesos en general.		
Aceptación		


Si		No	Parcial
----	---	----	---------


Verificar las preguntas que se deben realizar antes de brindar cualquier tipo de información
4. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No se evidencia en el documento de políticas de seguridad de la información algún punto que trate sobre llamadas telefónicas.
Aceptación
Si No  Parcial
Recomendaciones: Poseer una política de privacidad al momento de brindar datos sensibles


Investigar qué normas existen para el manejo de la documentación en los escritorios.
5. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No existe evidencia del manejo de estos documentos.
Aceptación
Si No  Parcial
Recomendaciones: Investigar políticas para manejar la documentación en los escritorios de la empresa


Verificar las sanciones aplicadas al incumplimiento de alguna de estas políticas.
6. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
Existe la restricción y manejo del acceso a las áreas con información de sensible, pero no se aborda el tema de las sanciones.
Aceptación
Si No  Parcial
Recomendaciones: Implementar una política para el cumplimiento de las sanciones

Solicitar la política de los sistemas de seguridad de las puertas de acceso restringido.
7. No cumple el requerimiento
Incumple la política del APO13.02 Gestionar un plan para el tratamiento del riesgo en la seguridad de la información.
Observación de la Administración
Existen controles de acceso manuales, pero no existe un control electrónico.
Aceptación
Si No Parcial 
Recomendaciones: La empresa cumple con disponer de controles para de acceso manual, pero no electrónico.


Solicitar reporte de personas que pueden acceder al área en concreto.
8. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No se evidencia la seguridad en el acceso en áreas comunes, solamente existe un control en áreas que contengan información sensible.
Aceptación
Si No  Parcial
Recomendaciones: Implementar algún mecanismo de seguridad para monitorear el acceso a las áreas comunes


Verificar que el espacio donde queda el dispositivo sea seguro
9. Cumple el requerimiento
Observación de la Administración
Se evidencia un control para la responsabilidad de la tenencia de los dispositivos tecnológicos hacia los empleados.
Aceptación
Si  No Parcial


Comprobar que el equipo se deje en un estado de suspensión o se encuentre apagado al momento de alejarnos del dispositivo
10. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No existe una evidencia del estado en el que quedan los dispositivos luego de su uso.
Aceptación
Si No  Parcial
Recomendaciones: La empresa deberá verificar el estado en el que quedan los dispositivos que no se usan en el momento.


Examinar que las redes de la empresa cumplan los estándares de seguridad de Wi-Fi.
11. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No existe una evidencia de que se utilice algún tipo de estándar de red para la conexión a Wi-Fi.
Aceptación
Si No  Parcial
Recomendaciones: Examinar los estándares de seguridad de Wi-Fi de las redes en la empresa.


Ejecutar chequeos periódicos para revisar si la información se filtra o se encuentra debidamente protegida.
12. Si se cumple el requerimiento
Observación de la Administración
Como mínimo cada mes, se realizar un chequeo para verificar la integridad de la información.
Aceptación


Si		No	Parcial
----	---	----	---------


Verificar el estado de las copias de seguridad, y chequear los dispositivos externos donde se almacenan los mismos.
13. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No hay documento que indique la verificación de las copias de seguridad, así como el chequeo de los dispositivos que almacenan esta información.
Aceptación
Si No  Parcial
Recomendaciones: Implementar mayores medidas de seguridad en las copias y análisis de los dispositivos externos en los que se almacena toda esta información.

Analizar los perfiles de los empleados capaces de realizar los backups para verificar que cumplan.
14. Se cumple el requerimiento
Observación de la Administración
Existe un documento que respalda el análisis de los perfiles con el permiso de realizar estas acciones de backup.
Aceptación
Si  No Parcial


Revisar los horarios de cierre de zonas restringidas que poseen información vital para la empresa.
15. No cumple el requerimiento
Incumple el APO13 Gestión de la seguridad
Observación de la Administración
No se dispone de los horarios para el cierre de zonas restringidas.
Aceptación
Si No  Parcial
Recomendaciones: La empresa debe asignar a un funcionario para lograr revisar los horarios a estas zonas restringidas anteriormente por la empresa.


Disponer de un guarda de seguridad o persona encargada de monitorear el acceso a estas zonas.
16. Se cumple el requerimiento
Observación de la Administración
Existe un control de acceso físico, a cargo del jefe de la unidad administrativa encargada de realizar el control.
Aceptación
Si  No Parcial

Revisar el tipo de información para ser clasificada y brindarle el tipo de seguridad que requiere de acuerdo con la necesidad de este.			
17. Se cumple el requerimiento			
Observación de la Administración			
Existe una política para cada tipo de información clasificada que se requiere administrar dentro de la empresa. Como por ejemplo políticas para administrar la información de base de datos, políticas para los backups, políticas para administrar las redes y demás áreas.			
Aceptación			
Si		No	Parcial

Verificar el tipo de seguridad que se va a brindar por categoría.			
18. Se cumple el requerimiento			
Observación de la Administración			
Se evidencia mediante un documento, donde se explica la forma de administrar los permisos de las personas que dispondrán del acceso a la información.			
Aceptación			
Si		No	Parcial

Hallazgos positivos

Ejecutar chequeos periódicos para revisar si la información se encuentra debidamente protegida.			
19. Si se cumple el requerimiento			
Observación de la Administración			
Una vez al mes, se ejecuta un chequeo para verificar la integridad de la información.			
Aceptación			
Si		No	Parcial

Guarda de seguridad encargada de vigilar el acceso a las áreas con información protegida.			
20. Se cumple el requerimiento			
Observación de la Administración			
En la empresa se dispone de una persona encargada de monitorear el acceso a las áreas que presentan información clasificada.			
Aceptación			
Si		No	Parcial


Conclusiones papel de trabajo:


En general, el área de seguridad de la información, la mayor parte de los hallazgos encontrados fueron conformes con un 50%, y la no conformidad con un 40% y un 10% parcial, por lo que muestra una ligera cantidad de hallazgos cumplidos, sin embargo, se deben mejorar también esos hallazgos negativos debido a la vital importancia de esto para el área de TI.


Los documentos que no se presentaron por parte del Hotel descanso en la montaña se exponen a continuación, evidencia de la utilización de una VPN, Política de privacidad para datos sensibles, documento para el manejo de documentación de los escritorios de la empresa, sanciones por el incumplimiento a cualquier política, no


existen controles de acceso electrónicos, no se encuentran políticas para el acceso a las áreas comunes, tampoco se encuentran la política para verificar el estados de los dispositivos al momento de terminar de usarlos, no existen estándares de seguridad con la red Wi-Fi, no hay manera de comprobar el estado de las copias de seguridad y de los dispositivos que almacenan esta información, y no existe un documento para revisar los horarios de cierre de las áreas restringidas.


Revisión de Software


Argumentos de la Auditoría Interna		
1. Según la sección tres, principios, apartado 3.5, seguimiento de los activos de Software, se verifica que se cuenta con un inventario actualizado de dichos activos de Software		
Observación de la Administración		
Si se cumple el aspecto a revisar ya que está presente la política de instalación y uso de Software		
Aceptación		
Si 	No	Parcial


Argumentos de la Auditoría Interna		
2. Se comprueba según el archivo que contiene la lista de Software autorizado por la empresa que si se cuenta con los programas a utilizar debidamente definidos		
Observación de la Administración		
Si se cumple el aspecto a revisar ya que está presente el inventario de Software actualizado.		
Aceptación		
Si 	No	Parcial


Argumentos de la Auditoría Interna		
3. No se presenta ninguna lista ni inventario que defina lo que la empresa toma como Software no autorizado		
Incumple con la política de uso de instalación de Software, en el punto 8, para gestionar el uso de Software libre y licenciado.		
Observación de la Administración		
No se cumple el aspecto, no existe manera de comprobar el requisito		
Aceptación		
Si	No 	Parcial
Recomendaciones: Según la política se debe tener una política de gestión del Software no utilizado.		


Argumentos de la Auditoría Interna
4. No cumple el requerimiento, debido a que no se presenta ninguna prueba específica que demuestre una actualización mensual o al incorporar Software nuevo.
Incumple con la política de uso de instalación de Software, en el punto 8, para gestionar el uso de Software libre y licenciado.
Observación de la Administración
Requisito no cumplido
Aceptación
Si No  Parcial
Recomendaciones: Ejecutar actualizaciones de las licencias y demás del Software utilizado en la empresa, para así mantener un óptimo proceso en el manejo de los datos.


Argumentos de la Auditoría Interna
5. No cumple con el requerimiento de mostrar un documento
Incumple con la política de uso de instalación de Software, en el punto 5, tener conocimiento sobre distribución y uso.
Observación de la Administración
La entrevista se llevó a cabo, pero no se cumple con el requisito de mostrar o proporcionar un documento donde se pueda verificar en cualquier momento la información otorgada por el entrevistado
Aceptación
Si No  Parcial
Recomendaciones: Manejar mediante algún documento la información revelada por los entrevistados, para tener la capacidad de consultarla en cualquier momento y lugar.


Argumentos de la Auditoría Interna
6. Si cumple el requerimiento
Observación de la Administración
Si se cumple el aspecto debido a que existe un documento que indica la existencia de un encargado que vela directamente la instalación de Software nuevo.
Aceptación
Si  No Parcial


Argumentos de la Auditoría Interna
7. Si cumple el requerimiento
Observación de la Administración
Según el artículo 3.3, una persona se encarga de verificar las licencias de los programas a instalar, además de verificar también los términos de la licencia.
Aceptación
Si  No Parcial

Argumentos de la Auditoría Interna
8. Se cumple el requerimiento
Observación de la Administración
Según el artículo 5.3, solo las personas con el rol delegado de T.I pueden instalar el Software
Aceptación
Si  No Parcial


Argumentos de la Auditoría Interna
9. No cumple con el requerimiento
Incumple con la política de uso de instalación de Software, tener conocimiento sobre distribución y uso.
Observación de la Administración
No hay pruebas que la empresa utilice un mecanismo o herramienta para detectar Software no autorizado en los equipos.
Aceptación
Si No  Parcial
Recomendaciones: Se le recomienda a la empresa implementar mecanismos para verificar la no existencia de Software no autorizado por la empresa.


Argumentos de la Auditoría Interna
10. No cumple con el requerimiento
Incumple con la política de uso de instalación de Software, responsabilidad y control.
Observación de la Administración
En el documento de las políticas no se encuentra ningún apartado que indique el proceso de investigación de incidentes.
Aceptación
Si No  Parcial
Recomendaciones: Se debe agregar alguna política que cumpla con las investigaciones de incidentes.

Argumentos de la Auditoría Interna
11. No cumple con el requerimiento
Incumple la política de la terminación de ciclo de vida del Software.
Observación de la Administración
A pesar de cumplir con registrar todas las licencias de Software, no hay manera de comprobar que se evalúe también las fechas de vencimiento y renovación de estas.
Aceptación
Si No  Parcial
Recomendaciones: La empresa deberá estar al pendiente de renovar las licencias del Software utilizado.

Argumentos de la Auditoría Interna
12. No cumple con el requerimiento establecido
Incumple con la política de uso de instalación de Software, responsabilidad y control.
Observación de la Administración
No existe ningún documento que informe acerca de la distribución de los gastos de las máquinas.
Aceptación
Si No  Parcial
Recomendaciones: Anotar la distribución de los gastos de las máquinas para adquirir una mayor capacidad en el control de estas.

Hallazgos Positivos

Actualización de inventario		
13. Se cumple el requerimiento		
Observación de la Administración		
Se mantiene siempre un buen control en la actualización del inventario		
Aceptación		
Si 	No	Parcial


Asignación de roles		
14. Se cumple el requerimiento		
Observación de la Administración		
Se define de manera adecuada y ordenada las tareas que debe realizar cada miembro de la organización.		
Aceptación		
Si 	No	Parcial


Conclusiones papel de trabajo:


En general, el área de revisión del Software, los hallazgos encontrados fueron conformes con un 50%, y la no conformidad fue de otro 50% lo que muestra un balance equitativo, sin embargo, se deben reforzar las áreas de no conformidad y presentar los documentos que no se presentaron, los cuales son los siguientes.


Política de gestión del Software no autorizado, actualizaciones de licencias, no se presenta un documento para la detección de Software no autorizado, no existe ninguna política de investigación de incidentes, documento que evidencie la distribución de gasto de las máquinas.


Seguridad Física


Ubicación segura del equipo en la empresa		
1. Cumple los requerimientos		
Observación de la Administración		
Según el documento entregado del Data Center del hotel el descanso, este cuenta con las instalaciones de hardware razonablemente seguras.		
Aceptación		
Si 	No	Parcial


Es una zona de poco tránsito, y no está próximo a ventanas.		
2. Cumple los requerimientos		
Observación de la Administración		
Según el documento del Data Center se puede observar que en esta área no existen ventanas próximas al lugar.		
Aceptación		
Si 	No	Parcial


Controles para el acceso a áreas específicas			
3. Cumple parcialmente los requerimientos			
Observación de la Administración			
Hay parcial conformidad, debido a que se confirma las tarjetas de acceso, pero no se encuentra información de bitácoras o registros, ni tampoco de cámaras de vigilancia y de controles biométricos.			
Aceptación			
Si	No	Parcial	


Trasporte del equipo autorizado por el personal de TI			
4. No cumple los requerimientos			
Incumple la política de gestión de activos			
Observación de la Administración			
No hay conformidad, debido a que en los documentos brindados no se encuentra esta información para el transporte del equipo.			
Aceptación			
Si	No		Parcial
Recomendaciones: Manejar de mejor manera el transporte del equipo.			


Prohibiciones para el transporte del equipo			
5. Cumple los requerimientos			
Observación de la Administración			
Hay conformidad, ya que se evidencia una política de uso del equipo fuera de la empresa por parte del empleado.			
Aceptación			
Si		No	Parcial


Prohibiciones consumir alimentos dentro de la empresa.			
6. Cumple los requerimientos			
Observación de la Administración			
Se evidencia en el documento de políticas de seguridad las prohibiciones mencionadas.			
Aceptación			
Si		No	Parcial


Medidas contra factores ambientales			
7. No cumple los requerimientos			
Observación de la Administración			
No hay conformidad, ya que el documento con esta información no fue proporcionado por la administración.			
Aceptación			
Si	No		Parcial


Sistema de seguridad del área del cuarto de servidores			
8. Cumple los requerimientos			
Observación de la Administración			
Según el documento del Data Center se puede observar que el lugar posee alarmas contra incendio, medidores de temperatura, detectores de humo y demás.			
Aceptación			
Si		No	Parcial


Equipos asegurados mediante una póliza.			
9. No cumple los requerimientos			
Observación de la Administración			
No hay conformidad, ya que el documento con esta información no fue proporcionado por la administración.			
Aceptación			
Si	No		Parcial

Contratos de mantenimiento de extintores.			
10. No cumple los requerimientos			
Observación de la Administración			
No hay conformidad, ya que el documento con esta información no fue proporcionado por la administración.			
Aceptación			
Si	No		Parcial


Contrato de extintores vigente.			
11. No cumple los requerimientos			
Observación de la Administración			
No hay conformidad, ya que el documento con esta información no fue proporcionado por la administración.			
Aceptación			
Si	No		Parcial

Participación de todo el personal en las capacitaciones del uso de extintores.			
12. Cumple parcialmente con los requerimientos			
Observación de la Administración			
Hay parcial conformidad, debido a que se presenta un documento con la asistencia a las capacitaciones por parte del personal, sin embargo, algunos empleados no asistieron a estas capacitaciones, por lo que no cumple el 100% de asistencia.			
Aceptación			
Si	No	Parcial	

Fotografías de los extintores del lugar.			
13. Cumple con los requerimientos			
Observación de la Administración			
Se presenta evidencia que muestra que efectivamente se han ubicado extintores en el área de TI.			
Aceptación			
Si		No	Parcial

Fotografías de paredes y techo del área de servidores
14. Cumple parcialmente los requerimientos
Observación de la Administración
Hay parcial conformidad, debido a que en el Data Center se evidencian las paredes del área de servidores, pero no del techo, tampoco se encuentra un documento para verificar que los materiales sean resistentes contra el fuego.
Aceptación
Si No Parcial 

Hallazgos Positivos

Alarmar contra incendios
15. Cumple con los requerimientos
Observación de la Administración
La empresa cuenta con adecuadas alarmas y alertas de humo en caso de incendio.
Aceptación
Si  No Parcial

Conclusiones papeles de trabajo:

En general, el área de Seguridad Física, los hallazgos encontrados fueron conformes con un 50%, y la no conformidad fue de otro 36% y un 14% de parcial conformidad, lo que muestra carencias que se deben mejorar urgentemente, además de presentar los documentos que no se presentaron, los cuales son los siguientes.

No se presenta evidencia de utilizar cámaras de vigilancia ni sistemas biométricos, no existe evidencia que respalde la seguridad del transporte del equipo empresarial, no se presenta un documento que muestre las normas ambientales a seguir, tampoco se encontraron evidencias de las pólizas para los trabajadores del lugar no hay evidencia del contrato de mantenimientos de extintores.

Conclusiones

El hotel durante la auditoria que se le realizo se logró obtener información que demostró que no cuenta con políticas internas que puedan generar un óptimo funcionamiento de algunas de las áreas, ya que en las peticiones realizadas hacia la empresa no toda la información se brindó, por lo que parte de las auditorías realizadas no se desarrollaron de la manera más optima.

También se encontraron inconsistencias en cuanto a los documentos de perfiles de trabajo, esto debido a perfiles que no existen en las políticas de puestos del hotel, y tampoco se presentan algunos documentos como el de vacaciones acumuladas.

El Hotel descanso en la montaña cumple con muchos de los requisitos y presentó la mayoría de los documentos solicitados, existen algunas inconsistencias, sin embargo, son totalmente mejorables, lo cual indica que este hotel dispone de una organización un tanto débil en aspectos como recursos humanos y seguridad de la información.

Bibliografía

- Material del curso: Auditoría de sistemas.
- Material proporcionado por el docente.