UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“PROPUESTA DE AUDITORIA DE RED, APLICANDO LA NORMA ISO 17799 PARA LA MEJORA DE SEGURIDAD DE DATOS EN LA CORPORACIÓN ACME. 2019-2020”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

GUARDIA CESPEDES, EDDER DARIO

ASESOR

OCHOA CARBAJAL, HERNÁN

Villa El Salvador

2019

DEDICATORIA

Para mi madre que siempre fue la inspiración, mi camino y mi guía para todo, Rocío Céspedes Sánchez, quién supo ser una madre perfecta, también para mi familia que supieron darme su apoyo ante cada circunstancia y siempre permanecieron a mi lado, dándome el impulso para seguir adelante.

AGRADECIMIENTO

Ante todo, a mi casa de estudios, Universidad Nacional Tecnológica de Lima Sur, que me guio el camino por el cual seguir y que, a su vez, me acogió como uno más de sus hijos durante un periodo que me permitió crecer de forma profesional.

A la Corporación Acme y Acme-Tic, por el apoyo y respaldo para desarrollar este trabajo, el cual me permitirá dar un paso más en mi carrera profesional.

Agradecer a todos los profesores que me brindaron su apoyo durante mi vida universitaria, en especial a los profesores de la carrera profesional de Ingeniería de Sistemas, quienes siempre brindaron sus consejos con la finalidad de formar grandes profesionales.

A mi asesor, el docente Hernán Ochoa Carbajal, quien desde la primera clase que llevamos juntos, me apoyó y aconsejó con la intención de que, al terminar la carrera, siempre siga hacia adelante.

Agradecimiento a todos los amigos que conocí en la universidad, aquellos que, con su sola presencia y ánimos, hicieron que sigamos avanzando sin detenernos.

Agradecer a mi familia, que siempre confiaron en mí y nunca dejaron que me quede sentado y me rinda.

A mis abuelos, que fueron unos excelentes padres para con mi madre, logrando así que esa forma de ver la vida llegue hacia mí y logre entender que la familia es siempre primero.

A mi pareja, que siempre está constantemente recordándome, que no debo quedarme atrás, que todo lo que haga siempre es un paso que me llevará para adelante.

LISTADO DE FIGURAS

LISTADO DE TABLAS

ÍNDICE

INTRODUCCIÓN

La auditoría de TI es un proceso sumamente importante que por lo general la mayoría de las empresas no tienen entre su lista de procedimientos, la realización de auditorías en lo que tecnología se trata, pues se prefiere realizar el cambio de las tecnologías sin importar muchas veces el costo o importancia que estas tienen.

Viéndose también que, si la empresa tuviera entre sus planes, realizar cada determinado tiempo, auditorias que permitan mantener un control de los equipos, ayudando no solo a su buen rendimiento, sino también permitiría prevenir y contrarrestar factores que puedan perjudicar a la empresa y generar perdidas ya sean económicas o de información.

Siendo considerado entre los activos principales, la información estaría encabezando la lista, pero dicha información principalmente se guarda en diversos equipos, ya sean en Pc Desktop o Servidores, pero que nos garantiza que los mencionados no corran riesgos de fallar y perder información única.

Además, realizando un proceso de auditoria con relación a la estructura de red en la que circula dicha información y se identifica problemas de las tecnologías que se manejan, lograríamos adelantarnos al problema y así evitar correr riesgos en cuanto a perdida de Data. Las tecnologías en una empresa, están diseñados para trabajar constantemente sin problemas bajo condiciones aceptables (corriente eléctrica estable, temperaturas no tan altas, uso aceptablemente correcto), pero en su mayoría, estas no son resistentes bajo múltiples problemas, lo cierto es que si tomamos como ejemplo un Router que es sometido a picos altos y cortes del fluido eléctrico, este podrá seguir trabajando, pero presentará problemas como, puertos dañados o pérdida de conexión, que se verían reflejadas en lentitud y pérdida al transferir datos.

Por lo que una auditoria constante sería una perfecta solución y prevención ante dichos problemas.

En el presente trabajo, el cual cuenta con 3 capítulos, se explica cada uno de los procesos de la propuesta, siendo el primer capítulo, el planteamiento del problema, logrando una descripción de la problemática en general, logrando que las fuentes de información relacionadas se muestren en el capítulo 2, que a su vez sirve como referencias y bases para desarrollar la propuesta en el capítulo 3, el cual a su vez, concluirá con recomendaciones a seguir.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

Las organizaciones se encuentran en una expansión económica y tecnológica en donde la información y el conocimiento son factores trascendentales para el desarrollo de su competitividad. Por tanto, para llegar a un conocimiento de calidad, las organizaciones deben asegurar que la información también sea de calidad y a su vez cuente con seguridad. Lo que se acaba de mencionar sólo se logra contando con procesos que contengan un nivel de madurez suficiente para mantener la cadena de valor de la información (desde los datos hasta la seguridad de estos), de manera que sean acordes y soporten la estrategia competitiva de la organización.

En la actualidad, el problema por pérdida o robo de información, se vuelve masiva, tal como se muestra a nivel global, sea el caso de robo de información personal, datos corporativos o incluso, información privada de gobiernos, originando que los niveles de protección para la información, se desarrollen de muchas formas, en nuestro caso, en el país, se sabe que no se realiza ningún tipo de actividad preventiva en contra de la perdida de información, en su gran mayoría, las empresas no toman conciencia hasta que se ven afectadas económicamente por perdida de información.

El departamento de Sistemas actualmente cuenta con una cantidad determinada de servicios al alcance de los usuarios de TI, pero la administración, control y monitoreo de estos servicios es cada vez mayor al igual que la difusión de estos a nivel de usuario de TI. Por lo expuesto anteriormente, es importante realizar las siguientes preguntas:

¿La información con la que cuenta la Corporación Acme, se encuentra realmente segura?

¿Qué debemos implementar para que la gestión de información dentro de la Corporación Acme sean de calidad y no se corra el riesgo de pérdida?

El diseño para trabajar será evaluado bajo la estructura que rige la norma ISO/IEC 17799:2017 “Código de Buenas Prácticas para la Gestión de la

Seguridad de la Información”, sobre este, se basará la generación de la propuesta de auditoria de red para la mejora de la seguridad de datos en la Corporación Acme.

Para realizar el análisis, se realizarán estudios del estado en el que se encuentran los procesos, dándole un enfoque prioritario a 3 características principales: Hardware, Software y Comunicaciones, estos serían evaluados mediante hallazgos de auditoria y formularios de reuniones, pero también trabajando en conjunto de herramientas para la auditoria como: entrevistas, cuestionarios y checklist.

1.2 Justificación del problema

La propuesta de auditoria de red para la mejora de la seguridad de datos en la Corporación Acme, basada en las recomendaciones de la norma ISO 17799, se logrará identificar la vulnerabilidad en la seguridad física y lógica de información, localizando debilidades en la red, permitiendo que estos puedan ser solucionados.

Por el aspecto económico, se reducirían gastos innecesarios causados por equipos o puntos defectuosos como: Switch o Router, como también, problemas lógicos originados por los ataques a los softwares usados, en cuanto al gasto, resulta mínimo, ya que, al identificar y solucionar los problemas, se podrán aprovechar en su totalidad los recursos internos para la Corporación Acme.

La Corporación Acme, durante lo poco más de 10 años que se encuentra en el mercado, cuenta con niveles de seguridad, que se vieron limitados con el pasar de los años, en el nivel lógico, los niveles de seguridad en relación de información, solo se ven minimizadas por el uso de antivirus, pero no en todos los ordenadores, estos problemas en conjuntos originan: perdida de data importante, fallas en la comunicación de equipos, sea a nivel de los medios de comunicación (cableado o inalámbrica), como a su vez posibles amenazas accidentales, como fallas del fluido eléctrico, problemas naturales(terrenos, mal clima), fallas por parte del personal, averías de hardware, problemas con el software; o también problemas intencionales: robo, fraude, mal uso de los equipos y mala gestión de la información.

Para el proceso de identificación de los puntos riesgosos o vulnerables a nivel físico y lógico en la Corporación Acme, la propuesta de auditoria bajo las normas de seguridad implementada por la ISO/IEC 17799 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

1.3 Delimitación del Proyecto

1.3.1 Teórica

Trabajaría bajo las normas de seguridad implementadas por la ISO/IEC 17799:2017 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”

1.3.2 Temporal

Inicio : septiembre de 2019
Fin : diciembre de 2019

1.3.3 Espacial

Se realizará en la sede de la Corporación Acme, ubicada en la Calle Los Sauces 325 San Isidro, a la espalda de la embajada de España.

1.4 Formulación del Problema

1.4.1 Problema General

- ¿Como se desarrollada la propuesta de auditoria de red para la mejora de la seguridad de datos en la Corporación Acme?

1.4.2 Problemas específicos

- ¿De qué manera la propuesta de auditoria de red para la mejora de la seguridad de datos, nos permitiría identificar los puntos vulnerables, con relación a la perdida de data en la Corporación Acme?
- ¿De qué manera la propuesta de auditoria de red para la mejora de la seguridad de datos, permite mejorar la integridad de la información en la Corporación Acme?

- ¿De qué manera la propuesta de auditoria de red para la mejora de la seguridad de datos permite mejorar la confiabilidad de la información en la Corporación Acme?

1.5 Objetivos

1.5.1 Objetivo General

Lograr que la Corporación Acme, forme parte de las empresas que, cuentan con una gestión de calidad, basada en un buen soporte de TI, generada por propuesta de auditoria de red para la mejora de la seguridad de datos en la Corporación Acme.

1.5.2 Objetivos Específicos

- Proponer una auditoria de red para la mejora de la seguridad de datos en la Corporación Acme, para la protección y prevención de data, se reducirían riesgos de perdida valiosa de información dentro de la Corporación Acme.

- Proponer una auditoria de red para la mejora de la seguridad de datos en la Corporación Acme, logrando reducir costos o sanciones, impuestas por los contratantes de los servicios de la Corporación Acme.

- Obtener un nivel de seguridad y confiabilidad de la información.

CAPITULO II: MARCO TEORICO

2.1. Antecedentes

2.1.1. Internacionales

Rivera y Zambrano, (2015). Realizó una auditoria llamada: *Auditoria al control y mantenimiento de la infraestructura tecnológica del departamento tecnológico de la espam mfl,* en la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. Al aplicar una auditoría al control y mantenimiento de la infraestructura tecnológica en el Departamento Tecnológico de la ESPAM MFL, nos da como permitido, la evaluación del nivel de los cumplimiento con respecto a las aplicaciones de buenas prácticas, estándares y normas de control interno de TI dentro de la Contraloría General del Estado Ecuatoriano, en relación con los políticas, procesos y procedimientos de los recursos tecnológicos (software y hardware) dentro de la entidad, se implementó la metodología determinada en las Normas Internacionales. 3 fases:

Planificación, tomando un estudio total de todos los elementos tanto internos y externos de la entidad, utilizando la evaluación de control interno en TI 410-09 y Norma ISO 27000 buscando obtener los hechos de mayor relevancia.

Durante la fase de Ejecución se aplicaron los procesos de auditoría, logrando mostrar los principales hallazgos ocasionados en la entidad.

Por último, la fase de Comunicación de Resultados se detallan todas las conclusiones y recomendaciones en relación a la presentación del Informe Final. Basándonos en los resultados obtenidos, se logra determinar que el área auditada lleva una dirección general de control y mantenimiento en la estructura tecnológica, pero se encuentra aplicada debidamente las normas mencionada con anterioridad, dando a relucir que el riesgo es alto y su confianza es bajo en los procesos, por lo que resulta conveniente la aplicación de dichas

normativas, permitiendo tomar mayor organización y responsabilidad, logrando minimizar los riesgos.

Cortes, (2016). Realizó un proyecto titulado: *Auditoría a la seguridad de la red de datos de la empresa Panavias S.A.,* en la Universidad Mayor de San Andrés. Como proyecto aplicado, tiene como meta el poder realizar la auditoría de seguridad en red de datos de la empresa Panavias S.A. en la ciudad de San Juan de Pasto, el cual busca por objetivo establecer controles y procedimientos con la finalidad de lograr establecer una gestión adecuada, permitiendo mostrar las vulnerabilidades y amenazas, mediante pruebas.

Para el desarrollo de la auditoria se aplicarán las cuatro fases:

La primera consiste en la recolección de la información pertinente a la red de datos, por medio de visitas técnicas guiadas y verificando la documentación existente a los procesos de servicio de red.

Durante la segunda fase de planeación, es donde son seleccionados los respectivos instrumentos de la auditoria que servirán para la recolección de información y las pruebas de penetración a ejecutar en la red de Panavias S.A., como también la normatividad a la aplicación en la presente auditoria.

En la tercera fase de ejecución, se aplicarán la instrumentaría seleccionada y las pruebas de penetración, con la finalidad de obtener puntos vulnerables existentes en la red de Panavias S.A., con los hallazgos se realizaría el análisis de riesgos para determinar que probabilidad y nivel de impacto que tienen estos riesgos sobre la red de datos.

En la cuarta y última fase, se realiza la organización de los resultados de la fase 3 y se determinaría los niveles de madurez, en relación a la normatividad seleccionada, realizándose una declaración de aplicabilidad, la cual contiene los controles y procedimientos con la finalidad de establecer un sistema de gestión adecuado.

Para finalizar, el informe final de la auditoria será entregado en la gerencia de la empresa Panavias S.A. para realizar las acciones indicadas.

Suárez, (2015). Realizó una implementación titulada: *Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización,* Universidad Nacional Abierta y Distancia. El trabajo describe principalmente los objetivos, el alcance, que expectativa tiene el SGSI y la metodología que se encuentra asociada a la definición, identificación diseño y planeación del modelo de seguridad de la información para Suárez Padilla & Cía Ltda, basados en la norma ISO 27001:2013; iniciando por analizar la situación actual de la organización desde la vista de los procesos críticos, identificación de los principales puntos débiles y amenazas, logrando aplicar una metodología de gestión del riesgos para la gestionar de los riesgos de seguridad de la información, planeación del plan a seguir para el trata de riesgos y producción del marco documental del sistema de gestión de seguridad de la información para Suárez Padilla & Cía Ltda.

El proyecto planteara la forma establecida de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). De acuerdo con las siguientes fases del proyecto:

- Descripción de la situación actual.
- Análisis de Riesgos.
- Identificación y valoración de todos los activos corporativos como partida de un análisis de riesgos.
- Identificación de las amenazas, evaluación y clasificación de las mismas.
- Evaluación del nivel de cumplimiento de la norma ISO/IEC 27002:2005.
- Obtención del Esquema Documental del sistema de gestión de seguridad de la información.
- Definir las Políticas, seleccionar los objetivos de control y los controles del anexo A de la norma ISO 27001; estableciendo una estrategia de contingencia.

Tola, (2015). Realizó una implementación titulada: *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001,* en la Escuela Superior Politécnica del Litoral. Se busca dar una solución adecuada para la seguridad de la empresa A&CGroup S.A., la cual parte de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), considerando el estándar de la norma ISO 27001:2005.

El primer capítulo, el marco teórico, se hace referencia a la revisión de los conceptos básicos que permitirán obtener una visión clara de las acciones necesarias, para que la entidad cuente con un sistema de seguridad y gestión de riesgos de la información.

Por otro lado, en el segundo capítulo, los antecedentes del proyecto hacen presencia, permitiendo que se describirá el problema, la solución, el objetivo general y los objetivos específicos.

El tercer capítulo, detalla el levantamiento de la información necesaria para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información).

El cuarto capítulo habla sobre la metodología PDCA (Plan – Do – Check - Act) y de los conceptos por cada etapa implicada en el modelo, también se detalla el alcance que se desea, indicando la dirección y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información

En el quinto capítulo se describe la metodología a seguir para la gestión del riesgo, tomando en cuenta los conceptos y ventajas principales al implementarlas, detallando el inventario de los activos de información dentro de la organización y se especifica el análisis de los riesgo con sus criterios de valoración; de igual forma se realizara la evaluación de los riesgos dentro del cual se procederá a describir la metodología usada para el cálculo de los valores de riesgo y la selección de las estrategias para el tratamiento de estos.

El desarrollo del sexto capítulo está centrado en la explicación al momento de implementar las políticas y el plan de tratamiento a seguir para la gestión de los riesgos que se encontraron.

En el séptimo capítulo sale a relucir el análisis de los resultados obtenidos y las técnicas de difusión que se usaron en la empresa.

2.1.2. Nacionales

Rafael y Castillo, (2017). Realizó un trabajo de implementación titulado: *Auditoria informática usando las normas COBIT en el Centro de Sistemas de Información del Hospital Regional Docente Las Mercedes de Chiclayo – 2016,* en la Universidad Pedro Ruiz Gallo. Que, mediante encuestas, checklist y entrevistas aplicadas, se observaron diversos problemas dentro de la gestión de TI, uno de los principales la congestión de diversos problemas en los sistemas y redes, que se dan de forma diaria en las áreas del Hospital Regional Docente Las Mercedes –HRDLM

Se detecto que el personal TI no sabe de todos los problemas que existen en las diversas áreas, cómo funciona los proceso y esto es por falta de supervisión constante.

El inminente peligro de pérdida de información en el HRDLM, por la falta de mecanismos de seguridad de la información.

Para lo cual se está utilizando COBIT versión 5, que nos apoya como guía de buenas prácticas en lo que respecta a la gestión de TI.

Para el desarrollo de la Auditoría se utilizó la metodología PHVA (Planificar, Hacer, Verificar y Actuar), lo cual permitió eliminar procesos repetitivos, logrando así reducir tiempos y mejoras en el análisis de cada proceso.

Una vez aplicada la evaluación se determinó que no existe un proceso que contrate, mantenga y motive los recursos humanos de TI, lo que genera la falta de personal dentro del área de TI, se sature con los diversos problemas que se generan. Además, si bien el área del CSI, cuenta con algunos controles que permiten verificar los procesos TI, hace falta que se realice una correcta supervisión para brindar un mayor aseguramiento de las políticas de la empresa.

Llegándose a desarrollar observaciones de manera detallada, fijándose riesgos por cada observación y generándose así, recomendaciones que ayuden a corregir las falencias encontradas.

Ramos, (2015). Realizó una propuesta de Plan de Auditoría Informática titulado: *Propuesta de un Plan de Auditoria Informática para el "Sistema de Información en Salud" y el "Aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015,* en la Universidad Nacional de Piura. Teniendo como objetivo proponer un plan de auditoría informática para los dos sistemas más importantes de cada establecimiento de salud, como el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.
Para ello, se ha planteado los siguientes objetivos específicos:

- Obtener conocimiento sobre la organización, normas y procedimientos de la Unidad Ejecutora 400 de la Región Piura donde se desarrollará la propuesta
- Establecer los objetivos de control y los procedimientos de auditoría que se aplicaran al Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.
- Determinar el programa de auditoría que se usara como indicador para la ejecución del Plan de Auditoría.

La idea de plan de auditoría informática se desarrolló, en base a la Guía de Control Interno de las entidades del Estado Peruano, la cual permite realizar un análisis de riesgos de los sistemas de información basándose en encuestas a los establecimientos de salud y a si vez se aplicó la Norma Técnica Peruana ISO 27001: 2008 con el objetivo de establecer las metas y procedimientos de control que se aceptan a los establecimientos de salud, permitiendo plasmarlo posteriormente en el programa detallado de auditoría informática.
Teniendo como finalidad el desarrollo de una guía para las futuras auditorías a los sistemas informáticos del estado peruano, tomando como origen la propuesta del plan de auditoría informática, logrando

también el monitoreo de los riesgos existentes relacionados al control de los procesos informáticos que llevan los sistemas.

Mariñas, (2015). Realizó una auditoria titulada: *Auditoría informática a la red de datos del Hospital de Tingo María para determinar la situación actual en la que se encuentra y proponer mejoras que garanticen el eficiente funcionamiento de la red corporativa,* en la Universidad Nacional Agraria de la Selva. El informe de auditoría está basado bajo el objetivo de desarrollar un estudio meticuloso en todo lo que puede estar ocasionando problemas en red y que, a su vez, pueden estar influyendo en la efectividad de los procesos del "Hospital de Tingo María".

Es por todos estos problemas que se observan, que se está buscando plantear una auditoria a nivel informático, de la red datos del Hospital de Tingo María y así poder determinar con certeza cual es la situación actual, para así proponer mejoras que logren garantizar el buen y eficiente funcionamiento de la red. Ya una vez que se cuente con los procesos de la auditoria debidamente aplicados, se procede con él análisis, evaluándolos a detalle, para luego comprarlo con la Norma Técnica Peruana NTP/ISO 17799:2007 y las Normas del Cableado Estructurado.

Logrando como resultado de la evaluación un el informe final de auditoría, en cual nos indica las deficiencias e infracciones que se encontraron durante el proceso, según la Norma Técnica Peruana NTP/ISO 17799: 2007 y las Normas de Cableado Estructurado.

Campos y Ríos, (2016). Realizó una auditoría titulada: *Auditoria en el uso de tecnología de información para optimizar la seguridad de Caja Sipan S.A,* en la Universidad Nacional Pedro Ruiz Gallo. El objetivo que se busca alcanzar, es la elaboración de la auditoría en relación con el uso de tecnología de información para la Caja Sipán S.A, teniendo como referencia el marco metodológico de lo estipulado como "buenas prácticas" en la Norma Técnica Peruana 17799, basada en la NTP ISO/IEC 17799:2007, también lo indicado en

Circular G-139-2009 – SBS, Circular G-140-2009 – SBS, Resolución S.B.S.N° 2116 - 2009, Reglamento de gestión operacional de la institución.

Al realizar el análisis del Sistema de Gestión de la Seguridad de la Información actual, permitió que el resultado obtenido apoye y permita determinar una adecuada acción gerencial, la definición de las prioridades para gestión de los riesgos dentro de la seguridad de la información y el implante de los controles elegidos para protegerse contra dichos riesgos.

Circular Nº G- 140 -2009: Gestión de la seguridad de la información y Resolución S.B.S. N° 2116 -2009: Reglamento para la gestión del riesgo operacional

2.2. Bases teóricas

SGSI (Sistema de Gestión de la seguridad de la Información)

Según lo indicado por la Organización Internacional de Normalización (ISO), un sistema de gestión de seguridad de información es como lo indica su nombre, un conjunto de información gestionadas mediante procedimientos que permitan mantener con un cierto nivel de seguridad a toda la información, esta tiene como base, el conjunto de elementos de la organización, logrando evaluar riesgos y fijar niveles.

(Buñay y Guanotuña2009, p.89)

Seguridad de la información

La información, forma parte de los activos más importantes del negocio, ya que la información se puede convertir en muchas cosas, entre ella progreso o decadencia, según como se use. Esto es muy importante en el ambiente interconectado de los negocios actual, la cual se va dando mediante el avanza de la tecnología, siendo a su vez que la información que se encuentra con mayor exposición cuente con mayor rango de amenaza. (NTP-ISO/IEC 17799,2007 p.5)

Auditoria

Siendo considerada como un proceso para la terminación del complimiento de las normas de las buenas prácticas, se indica además que este proceso puede ser realizado por cualquiera de las dos partes, donde el auditor, se encarga de auditar las actividades, software, hardware de la otra parte, que sería el auditado, según ISACA la auditoria de un sistema de información se puede definir como cualquier evaluación de todos los aspectos de los sistemas.
(NTP-ISO/IEC 12207, 2006 p.12)

Control interno de Información

Es el control diario para todas las actividades, con la finalidad de que sean realizadas con el cumplimiento de los procedimientos fijados por la Dirección de la Institución.

El control interno de información, suele ser un órgano dentro de la Dirección del Departamento de Informática, la cual tiene la misión, de asegurar que las medidas que se obtiene sean correctas y validad.
(Buñay y Guanotuña, 2009, p.35)

Estándar Internacional ISO/IEC 17799

La ISO/IEC 17799 es un estándar para la seguridad de la información, fue publicado originalmente como ISO/IEC 17799:2000 por la International Organization For Standardization, esta recomienda, el uso de mejores prácticas en la gestión relacionada con la seguridad de la información, para todo aquel interesado en mantener un estándar alto en lo que seguridad respecta.
(Cardoso y Zuluaga, 2007, p.28)

2.3. Definición de términos básicos

Hardware

Se hace referencia, a todos los dispositivos (objetos físicos), que conforman la estructura de un ordenador, como, por ejemplo, la placa madre, microprocesador, la memoria RAM, la fuente de poder, entre otros

(Cottino, 2009, p.15)

Software

Se muestra como el conjunto de programas, procedimientos y rutinas, las cuales se encuentran asociadas a una operación, la cual es ejecutada por el hardware.

(Cerón, 2014, p.19)

Norma Técnica

Son una serie de documentos que establecen los requisitos de calidad para el proceso de estandarización de los productos o servicios.

(Instituto Nacional de Calidad,2019)

PHVA

También conociendo como Ciclo Demin, siendo en español PHVA (Planificar - Hacer - Verificar - actuar), considerado principalmente como una estrategia, para la mejora continua.

(ESAN, 2016)

TI

Las TI o también llamadas Tecnologías De La Información y se le conocer como la utilización de tecnología, en lo general, computadoras, que facilitan un mejor manejo y procesamiento de la información.

(Economiatic, 2018)

ISO

Son las siglas en inglés International Organization for Standardization. Es la organización encargada de la normalización y estandarización, dedicándose

principalmente a la creación de normas para asegurar; calidad, seguridad y eficiencia de productos y servicios, conocidas comúnmente como Normas ISO.
(ISO. 2018)

Cableado Estructurado

Es un sistema de cables, conectores, canalizaciones y dispositivos de conexión, que permiten establecer una infraestructura de comunicación, que, por lo general, se encuentra dentro de un edificio.
(Perez y Gardey, 2014)

Seguridad de red

La seguridad de la red se enfoca en la prevención y protección de información, evitando la exposición o perdida no autorizada en redes corporativas, centrándose en dispositivos individuales, la seguridad de la red se encarga de verificar el cómo interactúan esos dispositivos y las conexiones entre ellos.
(Networkwolrd, 2018)

Data

Traducido a nuestro idioma, significa Datos, información, siendo un atributo, documento o información de algún tipo, relacionada a algo ya existente.
(Tecnologicon, 2018)

CAPITULO III: DESARROLLO DEL TRABAJO DE SUFICIENCIA PROFESIONAL

3.1. Modelo de solución propuesto

3.1.1. Proceso de Reconocimiento

La Corporación Acme se encuentra en un proceso de mejoras, que llegan de la mano con un crecimiento empresarial, esto dando paso a que sus exigencias a nivel de requerimientos o herramientas al momento de trabajar crezcan, es por eso que se ve en la necesidad de detectar y enfocar estrategias ligadas principalmente a la seguridad, siendo útiles para: las tecnologías, instalaciones de aplicativos y principalmente datos, siendo estas vulnerables o mal protegidas. A continuación, se detallarán algunas de las razones que indican el porqué es necesaria la auditoria propuesta:

- Constantes problemas de saturación a nivel del servidor de red, principalmente causados por falta de espacio (disco duro), por lo que el trabajo con la información resulta ser lento.
- Existen equipos que no cuentan con el antivirus instalado y configurado para trabajar de la mejor forma posible.
- El antivirus que se presenta instalado en los equipos, tiende a generar problemas en algunos otros softwares ya instalados, teniendo a su vez, problemas con las configuraciones fijadas por el administrador del área de TI.
- No se cuenta con el diseño original de la red, dando paso a que en el momento que se quiera desarrollar más puntos o mudar algunos, el seguimiento de estos resulte complicado.
- Los equipos que se van agregando a la red, ya sea cableada o inalámbrica, presentan problemas con el acceso a la red, generando problemas para el acceso de información, navegación o conexión con los demás equipos como las impresoras.
- No se cuenta bien aplicado el control de acceso a navegación.
- Los equipos de red, se apagan o reinician, debido a problemas en los puertos eléctricos.

- No se cuenta con una buena distribución de áreas que vayan acorde a los requerimientos.

El proceso de reconcomiendo se dividió de la siguiente manera:

3.1.1.1. Área de Hardware

No se cuenta con un control de fechas o periodos de mantenimiento preventivo, tampoco se puede constatar en qué estado se encuentran los diferentes equipos o cuales están para dar de baja y cuales se encuentran en garantía.

Se estima que en la Corporación Acme hay entre 95 a 100 equipos, encontrándose dentro de todos ellos, equipos como Desktop, Laptops, Servidores, Impresoras y fotocopiadoras.

No se cuenta con la cantidad de puntos eléctricos suficientes, ya que el número de usuarios va en aumento, causando el uso obligatorio de extensiones o supresores de pico, causando que estos queden expuestos a ser golpeados y apagar los equipos.

3.1.1.2. Área de Software

Se cuenta con aplicaciones que principalmente fueron desarrolladas a medida para cubrir con las exigencias de los procesos dentro de la Corporación Acme, a su vez, se cuentan con software adquiridos por el personal de TI, aparte de esos, existen los que llegan con los equipos al momento de ser adquiridos. Todos estos softwares, están distribuidos dentro de la Corporación Acme, cubriendo requerimiento.

Actualmente la Corporación Acme cuenta con las siguientes aplicaciones:

Sistemas Operativos (SO)			
Nombre	Versión	Origen	Ubicación
Windows 7	Sp 1	Lenovo Center	Desktop - usuarios
Windows 8	Sp 1	Lenovo Center	Laptop - usuario
Windows 10	1903	Lenovo Center	Desktop/Laptop - usuarios
Windows server 2016	-	Comprado	Servidor Aplicativos/BD
Windows server 2003	Sp2	Comprado	Servidor Dominio
Windows server 2012	-	Comprado	Servidor Correos
Mac OS	10.4	Fabricante	Laptop - Gerencia

Tabla 1 Sistemas Operativos (SO)
Fuente: Fuente Propia

Utilitarios más usados	
Nombre	Licencia
Office 365	Trimestral
GitHub	Anual
Visual Studio	Free
Adobe Reader	Free
Nitro Pro	Completa
VLC	Free
Winzip	Free
VueScan	Completa

Tabla 2 Utilitarios más usados
Fuente: Fuente Propia

Aplicativos a medida			
Nombre	Uso	Origen	BD
E-sam	Visualización de casos	PHP	SQL server
San-k	Control de casos	Visual Studio	SQL server
Central de llamadas	Registro de casos	Visual Studio	SQL server
Mantenimiento	Mantenimiento de casos	Visual Studio	SQL server
Informe Médico auditor	Informes de médicos externos	Visual Studio	SQL server
Higorr	Control Aduanero	PHP	SQL server
Central Audios	Escucha de llamadas	PHP	SQL server

Tabla 3 Aplicativos a medida
Fuente: Fuente Propia

Herramientas De TI		
Nombre	Proceso o uso	Descripción
Teamviewer	Todos los usuarios	Herramienta de soporte remoto
Bitdefender	60% de los usuarios	Control de Antivirus
Informes	Ejecutivos de Medi-k	Búsqueda de documentos
Solution Center	80% de los usuarios	Test de Equipos

Tabla 4 Herramientas TI
Fuente: Propia

3.1.1.3. Área de Comunicaciones

La Corporación Acme, actualmente cuenta con un dominio de red ACME.

La distribución de las Dirección IP, son la siguiente:

Asignación de IP's	
IP	Asignación
192.168.1.2	Servidor donde se encuentra instalado el Active Directory del dominio ACME
192.168.1.3/10	Servidores
192.168.1.11/40	Usuarios piso 1
192.168.1.41/50	Usuarios piso 2
192.168.1.51/60	Impresoras/fotocopiadoras
192.168.1.61/80	Equipos Wifi
192.168.1.81/100	Equipos piso 2
172.16.1.11/100	Telefonía IP

Tabla 5 Asignación de IP's Dominio ACME
Fuente: Fuente Propia

Entre los servidores, se tiene establecido las relaciones de confianza para su debida autentificación.

Todos los equipos se encuentran conectados a través de dos formas: cableada e inalámbrica. Siendo el caso de la inalámbrica, un problema ya que los equipos conectados por este medio, están limitados a una cantidad de conectados (20), ocupándose rápidamente al conectar celulares y laptops, también se presenta el problema de la señal, ya que, en determinados ambientes, la señal se pierde, puesto que el repetidor se encuentra en el centro del segundo piso.

En el caso de la red cableada, en el segundo piso, no se cuenta con los puntos necesarios para los usuarios.

La topología usada es del tipo Estrella, de tecnología Fast Ethernet y Protocolo TCP/IP.

El proveedor de internet, es FiberLux, el cual proporciona comunicación mediante fibra óptica, brindando también soporte en caso de problemas como: la conexión, velocidad, restricciones de navegación y algunos de los equipos de red brindados por ellos.

Equipos de comunicación		
Equipo	Marca	Modelo
Router	MikroTik	RB3011uias-RM
Router	MikroTik	RB2011uias-RM
Switch	3Com Baseline	2126-G
Switch	HP	48P JL382A
Router	Cisco	800 series
Convertidor	Raisecom	RC 512-FE-M
DVR	HikVision	DS7216HGHI-f1
UPS	Minuteman	ED6200RM
AccesPoint	Totolink	MT6200-CE
Almacenamiento	LinkStation	520D
Transceptor	Raisecom	RC001-1D

Tabla 6 Lista de Equipos de comunicación
Fuente: Fuente Propia

3.1.1.4. Estructura de la RED Corporación Acme

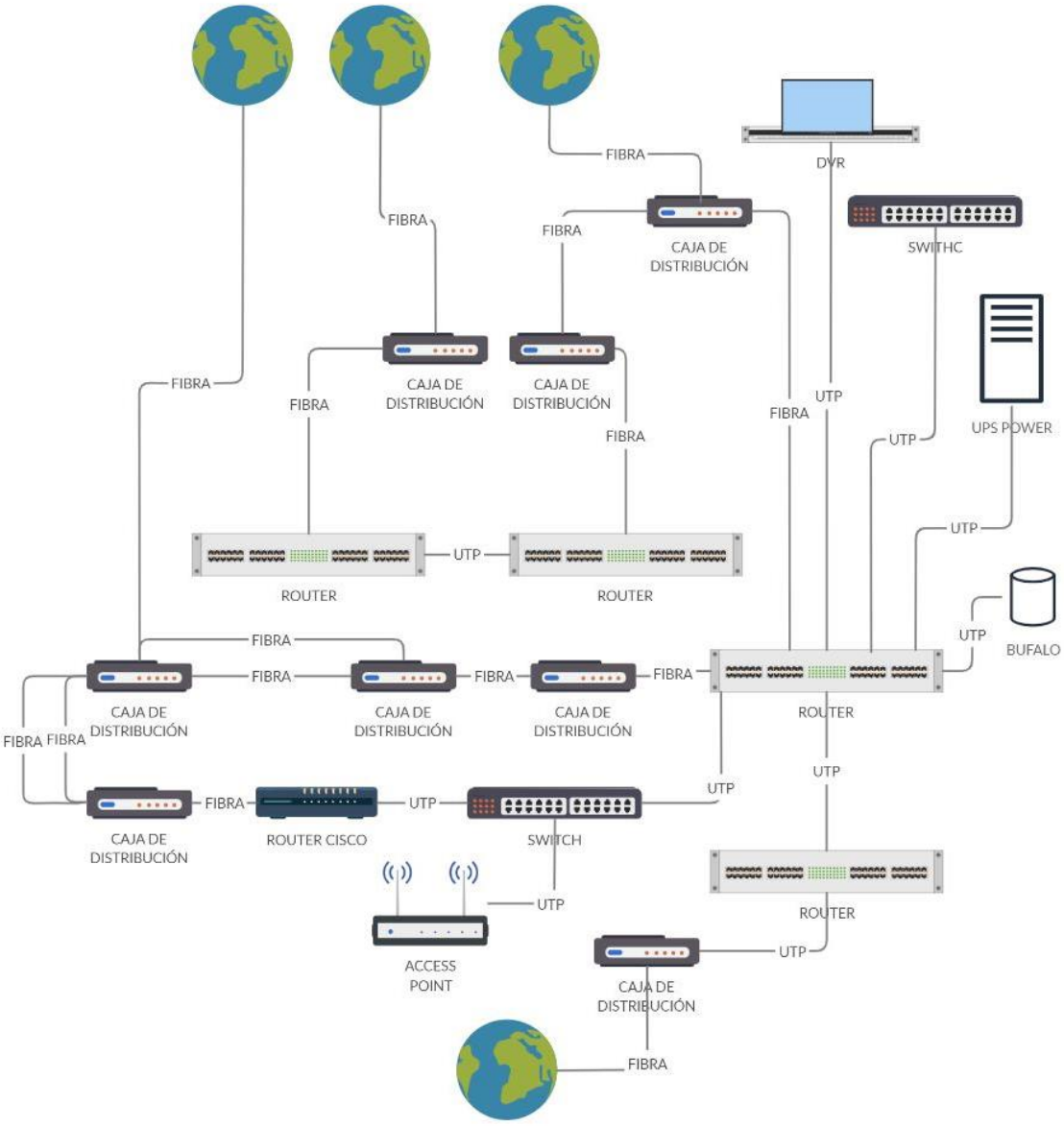

Figura 1 Estructura de Red Corporación Acme
Fuente: Fuente Propia

3.1.1.5. Ambientes

El espacio del Área de Sistemas no está distribuido de la mejor forma, ya que no se cuenta con un espacio designado solo para soporte, en el cual se puedan realizar mantenimientos preventivos, instalación, configuración, armados de equipos o reapariciones de tipo electrónica, dando lugar a que muchos de estas labores, se realicen en el lugar del usuario o del encargado.

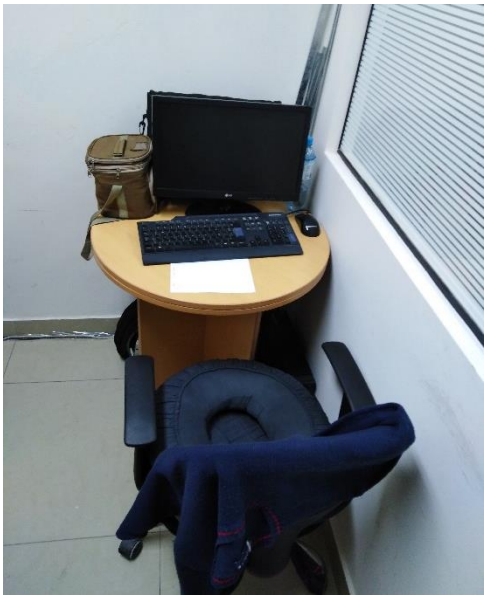

Figura 2 Poco espacio
Fuente: Fuente Propia

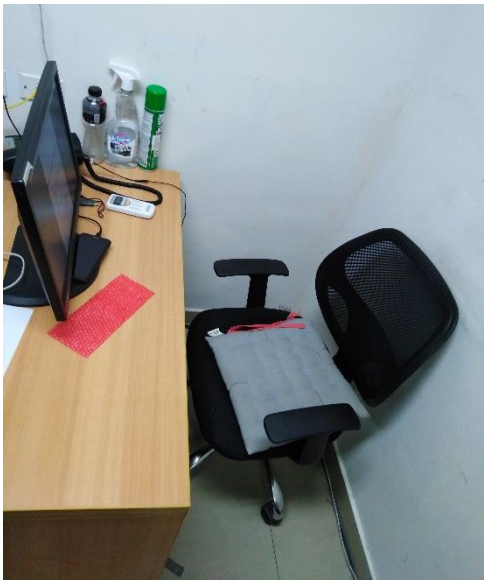

Figura 3 Poco espacio
Fuente: Fuente Propia

Fue por este mismo problema que el DataCenter, el cual se encontraba en un espacio de 2m x 1.15m, se terminó usando como lugar de almacenamiento para algunos equipos o parte de ellos. Antes del cambio de servidores, los cuales fueron mudados a un HOUSING, quedando solo routers y switch entre otros equipos, el data center se mantenía en un orden el cual permitía un mejor mapeo de cualquier problema, pero luego del cambio y los problemas eléctricos originados por el proceso de remodelación, se trabajó de forma no ordenada, originando que todo quede sin poder ser mapeado.

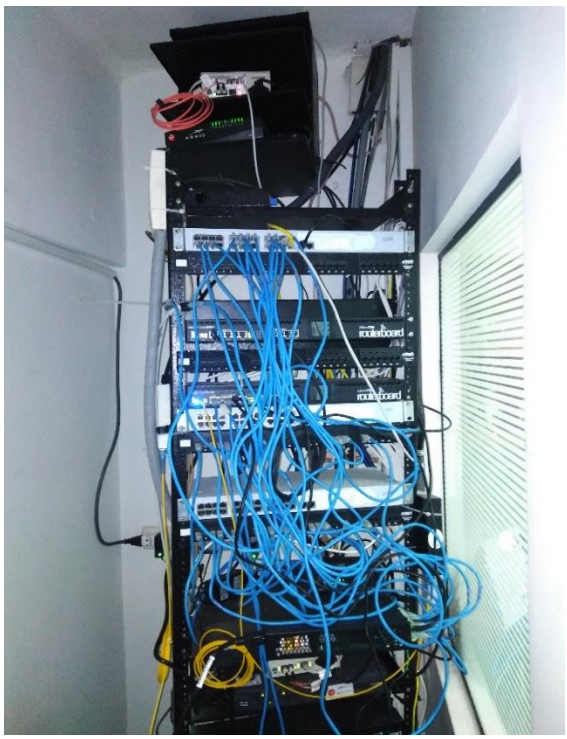

Figura 4 Desorden en el cableado
Fuente: Fuente Propia

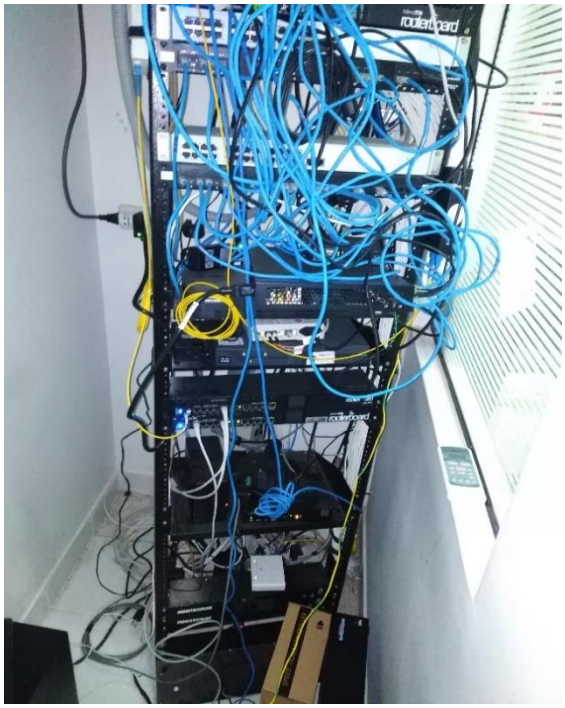

Figura 5 Desorden en los equipos
Fuente: Fuente Propia

Figura 6 Expuestos a caída y sin asegurar
Fuente: Fuente Propia

Figura 7 Notorio caso de falta en mantenimiento
Fuente: Fuente Propia

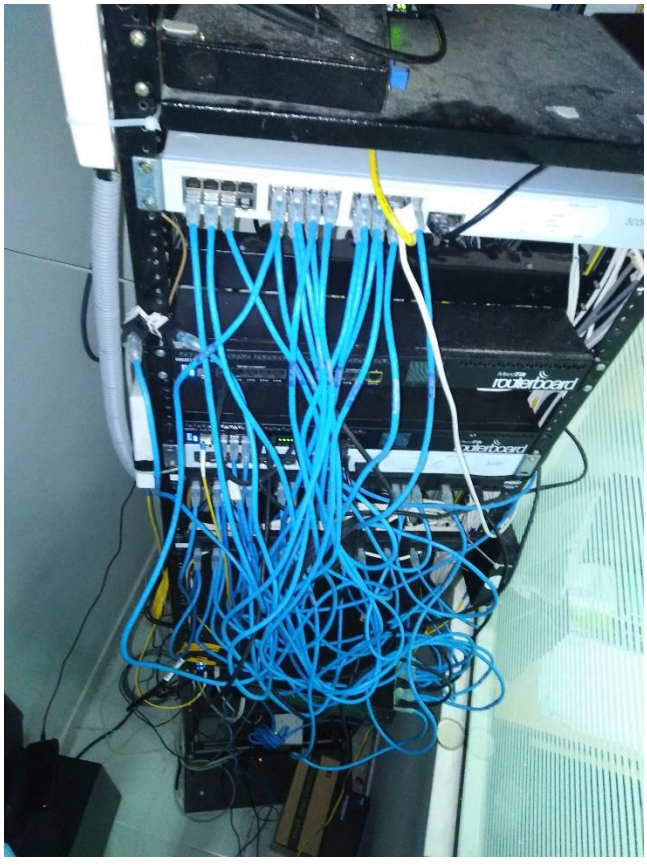

Figura 8 Cables en el piso expuestos
Fuente: Fuente Propia

3.1.2. Puntos vulnerables y amenazas

3.1.2.1 Humanas

En la siguiente tabla, se indica las vulnerabilidades y amenazas humanas, que podrían afectar los recursos informáticos de la Corporación Acme.

Área de Hardware	
Amenazas	Vulnerabilidades
Extracción no autorizada de equipos	No existe un control en la salida de equipo.
Fallas en el sistema eléctrico por trabajos (remodelación)	Equipos o componentes quemados.
Turbas o manifestantes	La ubicación de la Corporación Acme, cercana a muchas embajadas, por lo que se ve expuesta a ataques de manifestantes y otros.
Manipulación de equipos en el data center dentro de la Corporación Acme	Equipos malogrados por manipulación no apta o autorizada.
Gastos innecesarios por desconocimiento de existencia de garantía en equipos	Mala inversión en equipos innecesarios los cuales quedarían sin usar.
Equipos golpeados por negligencias	Perdida de equipos e información
Inexistencia de registros y calendarios de mantenimientos	Equipos presentando fallas técnicas
Equipos que se quedan sin reparación por diversas razones	Lentitud y atraso en el trabajo de los usuarios por falta y fallas de equipos.

Tabla 7 Lista de vulnerabilidades y amenazas humanas – área hardware
Fuente: Fuente Propia

Área Software	
Amenaza	Vulnerabilidad
No informar sobre las actualizaciones realizadas	Usuarios generando fallas durante el proceso de trabajo.
Ataques internos por mal uso de los recursos informáticos	Fallas en los sistemas y BD, que impidan realizar de forma normal los trabajos.
Falta de control y registros de los backups	Información perdida.
No se brinda soporte y administración de los aplicativos	No se cuenta con los manuales de los diferentes aplicativos.
Virus informáticos	Falta de antivirus en muchos equipos
Manipulación de aplicativos sin conocimiento o autorización	Usuarios sin capacitación o manuales que sirvan de guía para su uso.
Infección y propagación de virus	Uso inapropiado de internet y usb

Tabla 8 Lista de vulnerabilidades y amenazas humanas – área software
Fuente: Fuente Propia

Área comunicaciones	
Amenaza	Vulnerabilidad
Caída de la comunicación	Baja productividad
No se identifica los equipos con problemas	Fallas recurrentes y constantes caída de enlaces
Saturación de la red de trabajo	Sistemas lentos que atrasan el trabajo
Falta de administración en la red	Falta de capacitación para el control de la red laboral
Acces Point en lugares inseguros	Falta de conocimiento sobre la ubicación de los equipos de comunicación
Duplicidad en los IPs asignados	No se actualiza contantemente el registro de IPs
Mal uso y manipulación de los equipos de comunicación.	Mal ubicación de los equipos de comunicación

Tabla 9 Lista de vulnerabilidades y amenazas humanas – área comunicaciones
Fuente: Fuente Propia

3.1.2.2 Tecnológicas

En la siguiente tabla, se indica las vulnerabilidades y amenazas humanas, que podrían afectar los recursos informáticos de la Corporación Acme.

Área de Hardware y Software	
Amenazas	Vulnerabilidades
Ataques originados por código maliciosos	Falta de protección por carencia de antivirus y spam
Grabes daños en los sistemas	Falta de registro de las animalias en los diferentes sistemas (problemas, errores y advertencias)
Sabotaje interno	Carencia de control en el acceso a sistemas y BD

Tabla 10 Lista de vulnerabilidades y amenazas tecnológicas – área hardware y software
Fuente: Fuente Propia

Área Comunicaciones	
Amenazas	Vulnerabilidades
Equipos no activos por malas actualizaciones	No se cuenta con un control de los equipos de comunicación
Ataque de virus, malware, etc	Falla en la comunicación durante cualquier tipo de fallas.

Tabla 11 Lista de vulnerabilidades y amenazas tecnológicas – área comunicaciones
Fuente: Fuente Propia

3.1.2.3 Ambientales

En la siguiente tabla, se indica las vulnerabilidades y amenazas ambientales, que podrían afectar los recursos informáticos de la Corporación Acme.

Área Hardware y Software	
Amenazas	Vulnerabilidad
El área asignada a la DataCenter, está expuesta a polvo y humedad	Existencia de un ducto en el techo el cual está sin protección alguno
Si se llegara a inundar, es posible que los equipos se vean afectados por contar con cables en el suelo	Equipos guardados dentro del DataCenter, Ups y cables de datos
La humedad y smoke afectan a los componentes electrónicos de los equipos	El estar en un lugar como Lima que cuenta con un clima húmedo de lima y el gran congestionamiento vehicular

Tabla 12 Lista de vulnerabilidades y amenazas ambientales – área hardware y software
Fuente: Fuente Propia

Área comunicaciones	
Amenazas	Vulnerabilidades
Arboles altos que pueden cortar la fibra	Perdida de toda comunicación

Tabla 13 Lista de vulnerabilidades y amenazas ambientales – área comunicaciones
Fuente: Fuente Propia

3.1.3. Análisis de riesgos

Este identifica las amenazas, vulnerabilidades y riesgos, de la data en la organización con la finalidad de dar origen a un plan que asegure un ambiente estable y confiable, bajo los siguientes criterios: disponibilidad, confidencialidad e integridad de la data.

Durante el análisis se considerarán 2 puntos: la probabilidad de ser afectados por una amenaza y la magnitud del impacto que tendrá la amenaza, esta será medida por su nivel de degradación o su combinación de algunos elementos como la integridad, confidencialidad y disponibilidad.

La finalidad de saber sobre la existencia de estos riesgos, es el que hacer con ellos, teniendo como objetivos: mitigar, asumir y transferir los riesgos que nos puedan afectar.

- Mitigar los riesgos, con la implantación de normas y controles que ayuden a minimizar estos riesgos.
- Asumir los riesgos, a los que la organización se ve expuesta, ya que estos riesgos tienen como consecuencias un costo económico menor que el que sería aportar para la reducción de dichos riesgos.
- Transferir los riesgos, bien sea a una entidad especializada mediante su contratación.

Para este caso, se utilizará las NIST (Instituto Nacional de Estándares y Tecnología) Special Publication 800-30, el cual cuenta con 8 pasos para desarrollar el análisis:

- El sistema de caracterización:
- La identificación de las amenazas.
- La identificación de las vulnerabilidades.
- El análisis del control.
- La determinación de Riesgos.
- El análisis del impacto.
- La determinación de probabilidades.
- Las recomendaciones de los controles.

De no ser evaluados de forma imparcial y objetiva, el análisis realizado no cumpliría con la finalidad de ayudar a tomar las decisiones del cómo proteger los activos dentro de la Corporación Acme.

3.1.3.1. El sistema de caracterización (Paso 1)

Es la identificación del donde se realizará la evaluación de riesgos, sus límites del sistema de TI, los recursos y la información del sistema.

a) En el Sistema de TI, se detalla todo lo que forma parte de los sistemas de información, por ejemplo: el hardware, el software, los recursos de comunicación, los datos e información crítica, el personal que apoyan y utilizan el sistema de TI.

- En la tabla de Recursos de Hardware, se describen las características físicas principales de los servidores que mantienen los procesos dentro de la Corporación Acme.

Recursos de Hardware					
Marca	Modelo	Especificaciones	SO	IP	Asignación
HP	DL380G5	CPU xeon PIII 2.7Ghz / 4GB ram / Disco HP 72GB Sas 10K	Windows Server 2003	192.168.1.2	Dominio
Lenovo	X3250m	CPU Xeon E3 1240v6 3.70Ghz / 56GB ram / 4TB	Windows Server 2016	192.168.1.3	Base de Datos
Lenovo	X3250m	CPU Xeon E3 1240v6 3.70Ghz / 32GB ram / 2TB	Windows Server 2016	192.168.1.6	Aplicativos
HP	ML310G5	CPU Xeon E3110 3.0Ghz / 4GB ram / 1TB	Windows Server 2012	192.168.1.244	Correos

Tabla 14 Lista de los recursos de hardware
Fuente: Fuente Propia

- Recursos de Software, en la tabla se describen los sistemas instalados para mantener los procesos dentro de la Corporación Acme.

Recursos de Software			
Nombre	Uso	Origen	BD
E-sam	Visualización de casos	PHP	SQL server
San-k	Control de casos	Visual Studio	SQL server
Central de llamadas	Registro de casos	Visual Studio	SQL server
Mantenimiento	Mantenimiento de casos	Visual Studio	SQL server
Informe Médico auditor	Informes de médicos externos	Visual Studio	SQL server
Higorr	Control Aduanero	PHP	SQL server
Central Audios	Escucha de llamadas	PHP	SQL server

Tabla 15 Lista de los recursos de software
Fuente: Fuente Propia

- Herramientas de TI, en la tabla se describen las herramientas informáticas usadas dentro de la Corporación Acme.

Herramientas de TI		
Nombre	Proceso o uso	Descripción
Teamviewer	Todos los usuarios	Herramienta de soporte remoto
Bitdefender	60% de los usuarios	Control de Antivirus
Informes	Ejecutivos de Medi-k	Búsqueda de documentos
Solution Center	80% de los usuarios	Test de Equipos

Tabla 16 Lista de herramientas de TI
Fuente: Fuente Propia

- Sistemas Operativos, en la siguiente tabla se indican todos los sistemas operativos con los que cuenta la Corporación Acme.

Sistemas Operativos	
Nombre	Versión
Windows 7	Sp 1
Windows 8	Sp 1
Windows 10	1903
Windows server 2016	-
Windows server 2003	Sp 2
Windows server 2012	-
Mac OS	10.4

Tabla 17 Lista de sistemas Operativos
Fuente: Fuente Propia

- Recursos de comunicación, en la siguiente tabla se detalla todos los equipos relacionados a la comunicación dentro de la Corporación Acme.

Recursos de comunicación	
Equipo	Modelo
Router	RB3011uias-RM
Router	RB2011uias-RM
Switch	2126-G
Switch	48P JL382A
Router	800 series
Convertidor	RC 512-FE-M
DVR	DS7216HGHI-f1
UPS	ED6200RM
AccesPoint	MT6200-CE
Almacenamiento	520D
Transceptor	RC001-1D

Tabla 18 Lista de recursos de comunicación
Fuente: Fuente Propia

- Datos e información importante, en la tabla se detalla los recursos críticos de la Corporación Acme.

Datos e información importante	
Recurso	Descripción
BD SanK	Sistema de auditoria medica
BD Corporación Acme	Sistemas de RRHH
BD PYC	Sistemas de siniestros
Dwsank	Sistemas de reportes
Mantenimiento	Sistemas de mantenimiento de auditoria medica

Tabla 19 Lista de datos e información critica
Fuente: Fuente Propia

- Usuarios del sistema, son creados por petición de la gerencia, para posteriormente validar esta información en el equipo que se le designa, cuyos perfiles ya son de un Usuario Restringido.
- Personal que apoya los Sistemas de TI
  - Ing. Roosevelt flores
  - Ing. Luis González
  - Bach. Rolando Hidalgo
  - Bach. Carlos Sionchez
  - Bach. Kevin Quevedo
- Política de seguridad: actualmente la Corporación Acme, no ha implantado políticas de uso, ni ha informado a los nuevos usuarios el modo de trabajo con los ordenadores.
- Protección y almacenamiento de la información: no tiene ningún tipo que la salvaguarde y que mantenga su disponibilidad e integridad.
- Controles para el Sistema de TI: no se cuenta con normas de seguridad para los sistemas de TI.
- Entorno de la seguridad física: siendo el único nivel de seguridad, el personal de seguridad en el ingreso contratado por la misma Corporación Acme.

- Seguridad Ambiental de los sistemas TI: el DataCenter cuenta con su propio aire acondicionado, Ups y todos los equipos de Red y Comunicaciones. No se cuenta con un extintor propio, pero en caso de requerir se podrá utilizar el extintor del área de finanzas que es el más cercano.

b) Técnicas para la recolección de información

Para el proceso de recolección, se utilizaría:

- Cuestionarios
- Entrevistas: que, al obtener las respuestas, se encontrará los riesgos a los que se encuentran expuestos los recursos.

¿Qué puede estar mal en la Corporación Acme?

- Información perdida
- Equipos perdidos
- Producción reducida
- Ataques provocados
- Ataque a los servidores(hackers)
- Caiga de comunicación(enlaces)

¿Qué tan concurrentes son estos eventos?

- Tienden a ser de forma muy continua

¿Qué consecuencias traen estos eventos?

- Información perdida y sin recuperar
- Pérdida de tiempo, ya sea en reproducción o intentos de recuperación.
- Empleados dados de baja
- Problemas dentro de la institución

¿Qué tan dependiente es la Corporación Acme en relación con sus sistemas e información?

La Corporación Acme, no se encuentra preparada a realizar trabajos sin depender de los sistemas e información.

¿Qué cuenta con algún medio o proceso para identificar faltas por parte del personal?

- Faltas relacionadas a honestidad, no, pero si fallas durante sus labores al ingresas o trabajar casos, todo esto se posible al visualizarlos en el sistema.

¿Se cuenta con un nivel de confidencialidad y seguridad, para el acceso y manejos de los sistemas?

- No, los controlares de acceso a los diversos sistemas, cuentan con niveles de seguridad bajo.

- Revisión de los manuales relacionados a Ti: desafortunadamente la Corporación Acme, no cuenta con manuales que puedan ser de ayuda para el personal de TI o a los usuarios.
- Observación del ambiente: con la finalidad de lograr recolectar información del cómo se manejan los equipos, el entorno en el que se encuentran, la infraestructura de la red, etc.

3.1.3.2. La identificación de las amenazas y la identificación de las vulnerabilidades (Paso 2 y 3)

Estos pasos ya se encuentran agregados en el subcapítulo 3.1.2, en el cual se detallan las amenazas y vulnerabilidades en relación con la parte Humana, Tecnológica y Ambiental.

3.1.3.3. El análisis de control (Paso 4)

a) Control encontrado en Seguridad Física
   - Personal de seguridad contratado por la Corporación Acme.

b) Control encontrado en Seguridad Lógica

- Registro de los usuarios que acceden a los sistemas para el ingreso de información.

c) Control encontrado en RED

- No se encontró ningún control

3.1.3.4. Determinación de riesgos – probabilidad (Paso 5)

a) Probabilidad Alta

1. Resulta en pérdidas de los principales activos o recursos

2. Puede afectar de forma significativa a la organización al nivel de impedir el logo de la misión, la reputación e intereses.

3. Podría causar lesiones graves en el personal.

b) Probabilidad Media

1. Resulta en pérdida de materiales costosos de activos o recursos.

2. Puede afectar a la organización a nivel de impedir el logro de la misión, reputación e intereses.

3. Podría lesionar al personal.

c) Probabilidad Baja

1. Resultaría en la perdida de algunos materiales, activos o recursos.

2. Puede afectar en cierto grado a la organización.

Riesgos y Probabilidad	
Tipo de Riesgo	Probabilidad
Extracción de Data	Bajo-2
Fallas de los equipos	Medio-1
Fallas en el fluido eléctrico	Medio-1
Perdida de información	Alto-2
Virus	Alto-1
Perdida de comunicación	Bajo-1
Robo de las computadoras	Bajo-1
Robo de los servidores	Bajo-1
Robo de los equipos de comunicación	Medio-1
Robo de equipos de computo	Bajo-1
Inundación	Medio-1

Tabla 20 Riesgos y su Probabilidad
Fuente: Fuente Propia

Como se observa en la tabla 19, los riesgos son clasificados por el nivel de impacto o factor que genere. La clasificación se basaría en la importancia que estos riesgos presenten para la organización y la gravedad de pérdida si fuese el caso.

Para la cuantificación de los riesgos que conlleven a la pérdida de recursos, es factible asignar un valor dentro del rango de 0 a 10, tanto a la importancia que tenga el recurso, como al riesgo que tenga de ser perdido.

En la cuantificación se determinaría lo siguiente:

- La estimación del riesgo de perder el recurso.
- La estimación de importancia de los recursos.

Siendo el riesgo de un recurso (RR), el producto del Riesgo de pérdida (RP) por la Importancia del recurso (IR).

Ecuación n°1 $RR = RP * IR$

Para la evaluación de los riesgos mencionados en la tabla 19, se efectúa la Cuantificación de Riesgos

Cuantificación de los Riesgos		
Factor	Riesgo de Perdida - RP	Importancia del Recurso - IR
Baja	0	0
Media	5	5
Alta	10	10

Tabla 21 Cuantificación de los Riesgos
Fuente: Fuente Propia

	Hardware		
	Equipos de computo	Servidores	Router, Switch y Hubs
Robo	RR = 5*5 = 25	RR = 0*10 = 0	RR = 0*5 = 0
Conclusión por Robo	El riesgo de pérdida es medio bajo	El riesgo de pérdida es bajo	El riesgo de pérdida es bajo
Daño físico	RR = 10*5 = 50	RR = 10*10 = 100	RR = 0*5 = 0
Conclusión por daño físico	El riesgo de pérdida es medio	El riesgo de pérdida es alto	El riesgo de pérdida es bajo

Tabla 22 Cálculo de riesgo de pérdida - hardware
Fuente: Fuente Propia

	Software
	Información
Robo/Perdida/Sabotaje	RR = 5*10 = 50
Conclusión por Robo/Perdida/Sabotaje	El riesgo de pérdida es medio
Virus/Hackers/Sabotaje	RR = 10*10 = 100
Conclusión por Virus/Hackers/Sabotaje	El riesgo de pérdida es alto

Tabla 23 Cálculo de riesgo de pérdida – software
Fuente: Fuente Propia

	Comunicación		
	Enlaces de comunicación	La Red Inalámbrica	La Red LAN
Perdida de comunicación	RR = 10*10 = 100	RR = 10*10 = 100	RR = 5*10 = 50
Conclusión por perdida de comunicación	El riesgo de pérdida es alto	El riesgo de pérdida es alto	El riesgo de pérdida es medio
Desconexión de los cables de red			RR = 10*5 = 50
			El riesgo de pérdida es medio

Tabla 24 Cálculo de riesgo de pérdida – Comunicación
Fuente: Fuente Propia

3.1.3.5. Matriz de Riesgos: El Análisis de Impacto, La Determinación de Probabilidades y La Recomendaciones de los controles (Paso 6, 7 y 8)

Hardware							
Recursos	Amenazas	Vulnerabilidades	Control Existente	Impacto	Probabilidades	Nivel de Riesgo	Recomendaciones
Servidores	Mal uso	No se cuenta con políticas de uso	No existe un control	Alto	Alto	Medio	Establecer políticas para el uso de estos equipos
Computadoras	Mal uso	No se da a conocer las políticas de uso para estos equipos	No existe un control	Bajo	Bajo	Medio	Establecer políticas de uso, las cuales tienen que ser constantemente actualizadas y entregas
Laptops, impresoras, discos externos	Robo	No se cuenta con un control de salida para estos equipos	No existe un control	Bajo	Medio	Bajo	Reubicación de las cámaras que cuentan con puntos ciegos y un mejor control de salida
Equipos de computo	Que fallen	Fallas eléctricas	No existe un control	Alto	Alto	Alto	Análisis completo de todo el sistema eléctrico

Tabla 25 Matriz de Riesgos – Hardware
Fuente: Fuente Propia

Software							
Recursos	Amenazas	Vulnerabilidades	Control Existente	Impacto	Probabilidades	Nivel de Riesgo	Recomendaciones
Sistemas	Mal uso	Poco conocimiento por la parte usuaria	No existe un control	Alto	Alto	Alto	Capacitación para el buen manejo de los perfiles asignados
Datos	Perdida	No se da a conocer las políticas de uso para estos equipos	No existe un control	Alto	Alto	Alto	Establecer políticas de uso y control de los datos
Datos	Ataque	No se cuenta con un control de salida para estos equipos	No existe un control	Alto	Medio	Alto	Establecer políticas de uso que respalden la seguridad en el manejo de contraseñas
Base de datos	Mal uso	Fallas eléctricas	No existe un control	Alto	Alto	Alto	Capacitación constante para el buen manejo de la BD

Tabla 26 Matriz de Riesgos – Software
Fuente: Fuente Propia

Comunicaciones							
Recursos	Amenazas	Vulnerabilidades	Control Existente	Impacto	Probabilidades	Nivel de Riesgo	Recomendaciones
Rputer	Imperfectos	No se encuentran identificados	No existe un control	Alto	Bajo	Alto	Etiquetar para una buena identificación de los equipos
Switch	Imperfectos	No se encuentran identificados	No existe un control	Alto	Bajo	Alto	Etiquetar para una buena identificación de los equipos
Acces point	Imperfectos	Mala configuración para su finalidad	No existe un control	Bajo	Alto	Alto	Capacitar al encargado de los equipos para su buena configuración
Acces pint	Robo	Colocados sin ningún tipo de seguridad	No existe un control	Medio	Alto	Alto	Reubicación en puntos estratégicos y mejor seguridad al ser instalados

Tabla 27 Matriz de Riesgos – Comunicaciones
Fuente: Fuente Propia

3.1.4. Formulación de procesos y las herramientas a usar en el desarrollo de la auditoria

Los procesos formulados y las herramientas que se han determinado son:

Procesos:

- Formularios de Visitas
- Hallazgos de la Auditoria.

Herramientas:

- Entrevistas
- Checklist
- Cuestionarios

3.1.5. Diagrama del proceso de auditoria

Se muestra el método propuesto para el desarrollo de la auditoria.

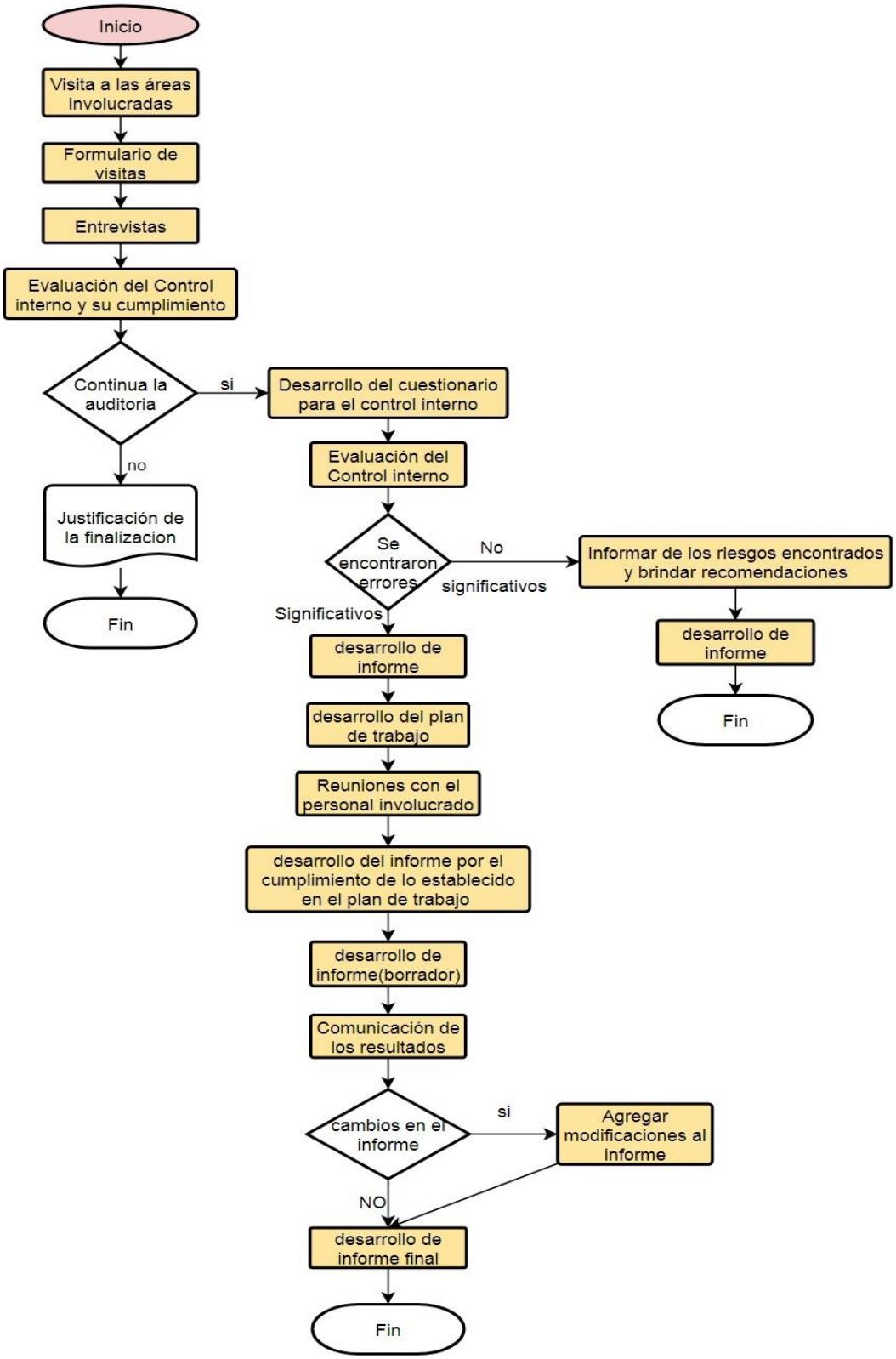

Figura 9 Diagrama del Proceso de Auditoria
Fuente: Fuente Propia

3.1.6. Plan de Trabajo

En la imagen se nuestro el plan de trabajo a seguir para la ejecución de la auditoria.

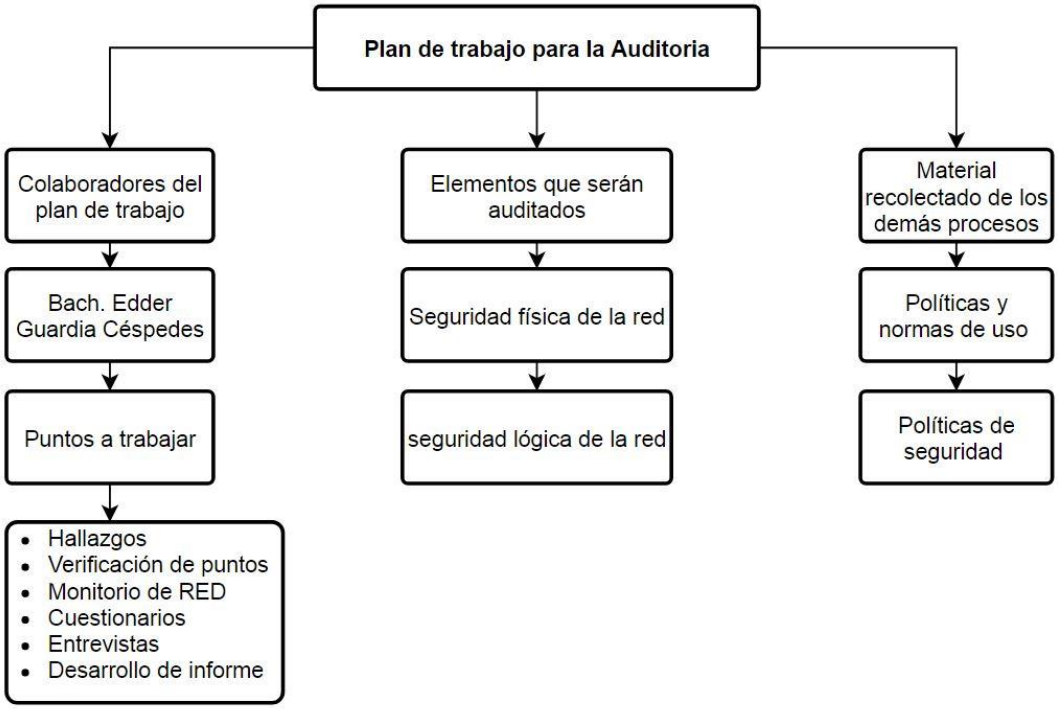

Figura 10 Plan de Trabajo
Fuente: Fuente Propia

3.2. Resultados

Se detallará los puntos observados, en relación a la seguridad de la red lógica y física.

3.2.1. Red Física

En el proceso de auditoria se encontraron las siguientes observaciones.

Puntos observados con relación al Hardware:

- El DataCenter, carece de un control para el acceso y detección de humo, según los estándares TIA/EIA-569-A.
- Mala distribución en la instalación de cables de datos y eléctricos.
- El aire acondicionado presente en el DataCenter, no se encuentra constantemente monitoreado, de manera que no se puede verificar su constante funcionamiento.

- Los cables no se encuentran correctamente identificados como lo indica la normal TIA/EIA-606.
- No se cuenta con el debido antivirus instalado en todos los ordenadores, exponiendo a una infección a todos los equipos en la red.
- No se realizaron análisis para definir la designación de equipos, de acuerdo a las funciones que va desempeñar el usuario.
- No se realiza de forma planificada el mantenimiento preventivo en los equipos de cómputo.
- Se desconoce el proceso del ingreso de un personal nuevo, generando desacierto al entregar un ordenador.
- Las tomas de corrientes presentan problemas en muchos casos, genera mala conexión y apagado del ordenador.

Puntos observados con relación al DataCenter:

- El DataCenter no cumple con las indicaciones de la normal TIA/EIA-569
- No cuenta con un control de acceso que mantenga alejado cualquier intento no autorizado de manipulación.
- No existe una debida identificación de los equipos.
- No se cumple con la norma TIA/EIA-606, ya que la el ducto de ventilación se encuentra sobre equipos.

Puntos observados en relación a Comunicaciones

- No se cuentan con herramientas suficientes para el mantenimiento de la red.
- No se realizan o se controlan, mantenimientos preventivos en los equipos de comunicación.
- Constante perdida de la comunicación.
- No existe un registro de equipos de comunicación.
- No se cuenta con un registro de los IPs.
- No se cuenta con la identificación de los puntos de comunicación.

3.2.2. Red Lógica

En el proceso de auditoria se encontraron las siguientes observaciones.
Puntos observados en relación a Software:

- Registro de fallas de los diferentes aplicativos desarrollados a medida para el desarrollo de funciones.
- Carencia de antivirus en diversos equipos.
- No se cuenta con una correcta designación de políticas de internet.
- Falta un mejor control de acceso a los Sistemas y BD
- No se cuenta con una clasificación de información.
- No se cuenta con un inventario de los recursos de Software
- Usuarios con un nivel bajo en conocimiento de sistemas.
- No se maneja un nivel alto con relación a la confidencialidad de contraseñas.
- No se cuenta con un registro de cambios o actualizaciones en los sistemas y aplicativos.
- Mal control y carencia de documentación de los backups.
- No existe un control documentado de almacenamiento de la información.

3.3. Instructivo de procedimientos

El instructivo esta desarrollado bajo la normal NTP-ISO/IEC 17799:2017 Código de Buenas Practicas para la Gestión de la Seguridad de la Información, la cual esta formada por once dominios o áreas, 39 objetivos de control y 133 controles, entre los cuales serán ajustados para las necesidades de la Corporación acmé, siendo esta la Seguridad física y lógica.
Una vez solucionado todos los puntos indicados en el instructivo, se podrá considerar como solucionado todo lo encontrado en la auditoria.

3.3.1. Política de seguridad

3.3.1.1 Seguridad lógica:

Este nivel debe comprende:

- Administración de acceso de usuarios

- Mantener un Registro de Usuarios, sus modificaciones, creaciones y eliminación.
- No permitir el acceso a la información, a usuarios no autorizados.
- El acceso a los equipos recién encendidos tiene que ser con un password.
- Los equipos que no se encuentren en uso por un determinado tiempo, tienen que pasar a un estado de suspensión, originando que se solicite la contraseña del usuario para volver a ingresar.

- Seguridad de Acceso de Terceros
  - Crear usuarios con un perfil que tenga restricciones, como si fueran auditores externos, personal temporal o pasantes.

- Control de Acceso a la Red
  - No permitir el mal uso del recuerdo “internet”, siendo usado de mala forma, como redes sociales o películas.
  - Constante monitoreo de la velocidad de internet.

- Control de Acceso a las Aplicaciones
  - Mantener un nivel de privacidad al momento de entregar las claves a los usuarios.
  - El password de Administrador de Red, solo tiene que se conocido por el personal encargado y el Administrador de Red.
  - Realizar cambios cada cierta fecha, de las contraseñas.
  - Las contraseñas de cuentas no tienen que ser usadas fuera de la institución
  - Generar contraseñas que mantengan un nivel alto de dificultad.

- No permitir el acceso a sistema a partir de ciertas horas.

- Monitoreo del Acceso y Uso del Sistema
  - Revisar constantemente las actualizaciones que la base de datos de virus esté trabajando.
  - Ejecutar solo los servicios necesarios para el buen funcionamiento de los servidores.
  - No instalar programas innecesarios en ordenadores o servidores.
  - No instalar sistemas operativos de un ordenador común en un servidor.

- Respaldo de Información (Servidores y Equipos de red)
  - Realizar la extracción de los backups según lo establecido en el calendario.
  - Realizar la copia de los backups en un lugar seguro.
  - Registrar el nombre del encargado que realiza estos procesos, también las características de los backups y su ubicación.
  - Realizar pruebas con los backups.

3.3.1.2 Seguridad Física:

- Ubicar los equipos de cómputo en lugares seguros.
- Deshabilitar periféricos innecesarios para el cumplimiento de las labores del personal.
- Colocar clave a la Bios del Equipo.
- Sujetar laptops con cables de seguridad.
- Mantener con seguridad de acceso, los equipos de comunicaciones.
- Reubicar los Acces Pointr en lugares más seguros y que a su vez tenga una mejor cobertura.
- Registrar los equipos que están para dar de baja y a su vez, los nuevos que entran de reemplazo.

- Mantener un inventario actualizado con las características de los equipos.
- Los equipos de cómputo, tienen que ser ubicado en lugares diseñados para ellos.
- Prohibir la ingesta de bebidas y comidas cerca de donde se encuentren los equipos.
- Los servidores solo estarán conectados al UPS.
- Prohibir el uso de tomas eléctricas defectuosas.
- Prohibir el uso de extensiones.
- Mantener un registro de los mantenimientos realizados y por realizar.
- Controlar el ingreso y salida de equipos dentro de institución.
- Prohibir el ingreso de elementos pirotécnico o cualquier otro que pueda generar fuego.
- Reordenar los equipos dentro del data centrar; router, switch y hubs.
- Etiquetar los equipos dentro del data center.
- El ingreso a la data center tiene que ser autorizado y registrado.
- No modificar la temperatura dentro del data center.
- Cumplir con el calendario de mantenimientos de los equipos de la data center.
- No meter a la data center, equipos que no tengan nada que ver con el data center.
- Todos los cambios que se realicen en relación a la red, ya sea cambio de equipos o configuraciones, tienen que ser registrados.
- Etiquetar todos los puertos en el patch panel, también cambiar los que se encuentren inoperativos.

3.4. Informe técnico basado en los resultados.

3.4.1 Informe preliminar

Ing. Roosvelt Florez

GRENTE DE ACME-TIC

De nuestra consideración:

Yo, Edder Guardia, me dirijo a usted con la intención de darle conocer el dictamen preliminar de la auditoría realizada a la Corporación Acme, la misma que se va llevado a cabo desde el 04 de octubre del presente año.

De los datos resultantes, me permito informarlas siguientes observaciones:

Red Física

En el proceso de auditoria se encontraron las siguientes observaciones.

Puntos observados con relación al Hardware:

- El DataCenter, carece de un control para el acceso y detección de humo, según los estándares TIA/EIA-569-A.
- Mala distribución en la instalación de cables de datos y eléctricos.
- El aire acondicionado presente en el DataCenter, no se encuentra constantemente monitoreado, de manera que no se puede verificar su constante funcionamiento.
- Los cables no se encuentran correctamente identificados como lo indica la normal TIA/EIA-606.
- No se cuenta con el debido antivirus instalado en todos los ordenadores, exponiendo a una infección a todos los equipos en la red.
- No se realizaron análisis para definir la designación de equipos, de acuerdo a las funciones que va desempeñar el usuario.
- No se realiza de forma planificada el mantenimiento preventivo en los equipos de cómputo.
- Se desconoce el proceso del ingreso de un personal nuevo, generando desacierto al entregar un ordenador.

- Las tomas de corrientes presentan problemas en muchos casos, genera mala conexión y apagado del ordenador.

Puntos observados con relación al Data Center:

- El Data Center no cumple con las indicaciones de la normal TIA/EIA-569
- No cuenta con un control de acceso que mantenga alejado cualquier intento no autorizado de manipulación.
- No existe una debida identificación de los equipos.
- No se cumple con la norma TIA/EIA-606, ya que la el ducto de ventilación se encuentra sobre equipos.

Puntos observados en relación a Comunicaciones

- No se cuentan con herramientas suficientes para el mantenimiento de la red.
- No se realizan o se controlan, mantenimientos preventivos en los equipos de comunicación.
- Constante pérdida de la comunicación.
- No existe un registro de equipos de comunicación.
- No se cuenta con un registro de los IPs.
- No se cuenta con la identificación de los puntos de comunicación.

Recomendaciones:

Hardware

En relación a los puntos observados con respecto al hardware, se recomienda lo siguiente:

- Rediseñar el cableado estructurado tomando en cuenta el estándar de la norma TIE/EIA 568-B2, TIA/EIA 569-B, TIA/EIA 606A y TIA/EIA 607
- El fluido eléctrico y de comunicación que llega a los servidores, tiene que ser bien instalados y fijados, durante la instalación, estos no deben tener cercanía.

- Elaborar la documentación que indique el diseño que se siguió para el proceso de instalación.
- Proteger los equipos de posibles fallas en el aire acondicionado.
- Realizar mantenimientos preventivos a los equipos de aire acondicionado, llevando un registro en el que se pueda controlar fechas y lo que se realizó.
- Manejar el ingreso y egreso de nuevos y viejos equipos, los cuales conformarían la lista de ordenadores de la institución.
- Coordinar con el área de RRHH, las cual tendrá que avisar con anticipación la contratación de nuevo personal, permitiendo tener listo espacio y equipo para su uso, según su función a desempeñar.
- Desarrollar y mantener actualizado el inventario de los activos importantes asociados a los sistemas, identificándolos y enumerándolos.
- Generar una base de datos con los controles de fechas importante, como periodos de mantenimiento, actualizaciones, modificaciones y garantías.

Data Center:

En relación a los puntos observados con respecto al Data Center, se recomienda lo siguiente:

- Modificar el espacio del Data Center según lo indicado por la normal TIA/EIA-569-B.
- Verificar y dar mantenimiento al USP del Data Center.
- Colocar Indicaciones que prohíban ciertas actividades dentro o cerca del Data Center.
- Realizar un mantenimiento completo dentro del Data Center para eliminar cualquier elemento que pueda perjudicar el funcionamiento de los equipos.
- Capacitar a todo el personal del área de Sistemas para un mejor uso y manipulación de los equipos en el Data Center.
- Etiquetar los equipos dentro del data center.
- Instalar un control de acceso.

Comunicaciones:

En relación a los puntos observados con respecto a Comunicaciones, se recomienda lo siguiente:

- Comprar herramientas que permitan trabajar y detectar problemas en la red.
- Realizar el mantenimiento preventivo a todos los equipos de comunicación.
- Etiquetar los equipos de comunicación.
- Realizar una evaluación de usuarios con la finalidad de ver, si es necesario el uso de internet para sus labores.
- Desarrollar e implementar normas para el uso del internet.
- Realizar el registro de las asignaciones de ip.
- Redistribuir los equipos, según las necesidades de las funciones de cada usuario.

Red Lógica

En el proceso de auditoria se encontraron las siguientes observaciones.

Puntos observados en relación a Software:

- Registro de fallas de los diferentes aplicativos desarrollados a medida para el desarrollo de funciones.
- Carencia de antivirus en diversos equipos.
- No se cuenta con una correcta designación de políticas de internet.
- Falta un mejor control de acceso a los Sistemas y BD
- No se cuenta con una clasificación de información.
- No se cuenta con un inventario de los recursos de Software
- Usuarios con un nivel bajo en conocimiento de sistemas.
- No se maneja un nivel alto con relación a la confidencialidad de contraseñas.
- No se cuenta con un registro de cambios o actualizaciones en los sistemas y aplicativos.
- Mal control y carencia de documentación de los backups.
- No existe un control documentado de almacenamiento de la información.

En relación a los puntos observados con respecto a la Red Lógica, se recomienda lo siguiente:

- Registrar las fallas en los sistemas, para así poder brindar un apoyo adecuado a la parte usuaria y a su vez tener precedentes que sirvan para prevenir fallas nuevas, permitiendo un buen funcionamiento como lo indica la norma ISO 1799:2007.
- Adquirir licencias suficientes de antivirus para todos los equipos dentro de la institución.
- Mantener un control de cambios de los sistemas.
- Coordinar con el área de RRHH para la previa instalación de los sistemas que pueda usar un nuevo trabajador.
- Adquirir herramientas para el monitoreo de equipos y redes.
- Establecer políticas de control en el acceso a los aplicativos según el perfil del usuario.
- Desarrollar e implementar políticas para el manejo de los backups, en el cual se detalle características del mismo, fechas, ubicación y encargado, tal como lo indica la norma ISO 1799:2007.
- Iniciar la migración a sistemas operativos más actuales, los cuales permitan trabajar conjuntamente con las actualizaciones en los sistemas.
- Desarrollar e implementar un inventario sobre los recursos de software; aplicativos, herramientas de desarrollo, utilitarios, todo esto según como lo detalla la norma ISO 17799:2007.

3.4.2. Informe final

Una vez terminado el plazo de dar a conocer las modificaciones que se tienen que realizar por parte de la gerencia, al no existir ningún cambio, se procede a redactar el informe final.

Ing. Roosvelt Florez

GRENTE DE ACME-TIC

De nuestra consideración:

Yo, Edder Guardia, me dirijo a usted con la intención de darle conocer el dictamen preliminar de la auditoría realizada a la Corporación Acme, la misma que se va llevado a cabo desde el 04 de Octubre del presente año.

De los datos resultantes, me permito informarlas siguientes observaciones:

Red Física

En el proceso de auditoria se encontraron las siguientes observaciones.

Puntos observados con relación al Hardware:

- El DataCenter, carece de un control para el acceso y detección de humo, según los estándares TIA/EIA-569-A.
- Mala distribución en la instalación de cables de datos y eléctricos.
- El aire acondicionado presente en el DataCenter, no se encuentra constantemente monitoreado, de manera que no se puede verificar su constante funcionamiento.
- Los cables no se encuentran correctamente identificados como lo indica la normal TIA/EIA-606.
- No se cuenta con el debido antivirus instalado en todos los ordenadores, exponiendo a una infección a todos los equipos en la red.
- No se realizaron análisis para definir la designación de equipos, de acuerdo a las funciones que va desempeñar el usuario.
- No se realiza de forma planificada el mantenimiento preventivo en los equipos de cómputo.

- Se desconoce el proceso del ingreso de un personal nuevo, generando desacierto al entregar un ordenador.
- Las tomas de corrientes presentan problemas en muchos casos, genera mala conexión y apagado del ordenador.

Puntos observados con relación al Data Center:

- El Data Center no cumple con las indicaciones de la normal TIA/EIA-569
- No cuenta con un control de acceso que mantenga alejado cualquier intento no autorizado de manipulación.
- No existe una debida identificación de los equipos.
- No se cumple con la norma TIA/EIA-606, ya que la el ducto de ventilación se encuentra sobre equipos.

Puntos observados en relación a Comunicaciones

- No se cuentan con herramientas suficientes para el mantenimiento de la red.
- No se realizan o se controlan, mantenimientos preventivos en los equipos de comunicación.
- Constante pérdida de la comunicación.
- No existe un registro de equipos de comunicación.
- No se cuenta con un registro de los IPs.
- No se cuenta con la identificación de los puntos de comunicación.

Recomendaciones:

Hardware

En relación a los puntos observados con respecto al hardware, se recomienda lo siguiente:

- Rediseñar el cableado estructurado tomando en cuenta el estándar de la norma TIE/EIA 568-B2, TIA/EIA 569-B, TIA/EIA 606A y TIA/EIA 607
- El fluido eléctrico y de comunicación que llega a los servidores, tiene que ser bien instalados y fijados, durante la instalación, estos no deben tener cercanía.

- Elaborar la documentación que indique el diseño que se siguió para el proceso de instalación.
- Proteger los equipos de posibles fallas en el aire acondicionado.
- Realizar mantenimientos preventivos a los equipos de aire acondicionado, llevando un registro en el que se pueda controlar fechas y lo que se realizó.
- Manejar el ingreso y egreso de nuevos y viejos equipos, los cuales conformarían la lista de ordenadores de la institución.
- Coordinar con el área de RRHH, las cual tendrá que avisar con anticipación la contratación de nuevo personal, permitiendo tener listo espacio y equipo para su uso, según su función a desempeñar.
- Desarrollar y mantener actualizado el inventario de los activos importantes asociados a los sistemas, identificándolos y enumerándolos.
- Generar una base de datos con los controles de fechas importante, como periodos de mantenimiento, actualizaciones, modificaciones y garantías.

Data Center:

En relación a los puntos observados con respecto al Data Center, se recomienda lo siguiente:

- Modificar el espacio del Data Center según lo indicado por la normal TIA/EIA-569-B.
- Verificar y dar mantenimiento al USP del Data Center.
- Colocar Indicaciones que prohíban ciertas actividades dentro o cerca del Data Center.
- Realizar un mantenimiento completo dentro del Data Center para eliminar cualquier elemento que pueda perjudicar el funcionamiento de los equipos.
- Capacitar a todo el personal del área de Sistemas para un mejor uso y manipulación de los equipos en el Data Center.
- Etiquetar los equipos dentro del data center.
- Instalar un control de acceso.

Comunicaciones:

En relación a los puntos observados con respecto a Comunicaciones, se recomienda lo siguiente:

- Comprar herramientas que permitan trabajar y detectar problemas en la red.
- Realizar el mantenimiento preventivo a todos los equipos de comunicación.
- Etiquetar los equipos de comunicación.
- Realizar una evaluación de usuarios con la finalidad de ver, si es necesario el uso de internet para sus labores.
- Desarrollar e implementar normas para el uso del internet.
- Realizar el registro de las asignaciones de ip.
- Redistribuir los equipos, según las necesidades de las funciones de cada usuario.

Red Lógica

En el proceso de auditoria se encontraron las siguientes observaciones.

Puntos observados en relación a Software:

- Registro de fallas de los diferentes aplicativos desarrollados a medida para el desarrollo de funciones.
- Carencia de antivirus en diversos equipos.
- No se cuenta con una correcta designación de políticas de internet.
- Falta un mejor control de acceso a los Sistemas y BD
- No se cuenta con una clasificación de información.
- No se cuenta con un inventario de los recursos de Software
- Usuarios con un nivel bajo en conocimiento de sistemas.
- No se maneja un nivel alto con relación a la confidencialidad de contraseñas.
- No se cuenta con un registro de cambios o actualizaciones en los sistemas y aplicativos.
- Mal control y carencia de documentación de los backups.
- No existe un control documentado de almacenamiento de la información.

En relación a los puntos observados con respecto a la Red Lógica, se recomienda lo siguiente:

- Registrar las fallas en los sistemas, para así poder brindar un apoyo adecuado a la parte usuaria y a su vez tener precedentes que sirvan para prevenir fallas nuevas, permitiendo un buen funcionamiento como lo indica la norma ISO 1799:2007.
- Adquirir licencias suficientes de antivirus para todos los equipos dentro de la institución.
- Mantener un control de cambios de los sistemas.
- Coordinar con el área de RRHH para la previa instalación de los sistemas que pueda usar un nuevo trabajador.
- Adquirir herramientas para el monitoreo de equipos y redes.
- Establecer políticas de control en el acceso a los aplicativos según el perfil del usuario.
- Desarrollar e implementar políticas para el manejo de los backups, en el cual se detalle características del mismo, fechas, ubicación y encargado, tal como lo indica la norma ISO 1799:2007.
- Iniciar la migración a sistemas operativos más actuales, los cuales permitan trabajar conjuntamente con las actualizaciones en los sistemas.
- Desarrollar e implementar un inventario sobre los recursos de software; aplicativos, herramientas de desarrollo, utilitarios, todo esto según como lo detalla la norma ISO 17799:2007.

Nota: El Ing. Roosvelt Florez, firma como constancia al estar de acuerdo con lo encontrado y lo recomendado.

CONCLUSIONES

- Mediante el presente trabajo, se dieron a conocer diversos puntos que se mostraban como grandes riesgos para la seguridad física y lógica dentro de la Corporación Acme.

- Los riesgos mostrados mediante el análisis de riesgos, detallaron de forma profunda los puntos a solucionar, detectando las amenazas y vulnerabilidades a las cuales se encuentra expuesta, también indicando la probabilidad que tienen estas de ocurrir y su grado de riesgo de cada una.

- Nos niveles de seguridad física y lógica no son los mas aptos, dando lugar a que ocurran muchas fallas durante el proceso de trabajo.

- Muchos de los procesos que se realizan no cumplen con los principios de seguridad de la información.

- Todo lo encontrado, fue gracias al proceso de auditoría, cuestionarios y entrevistas, las cuales fueron las herramientas usadas dura el trabajo de recolección, permitiendo mostrar las carencias de seguridad en la Corporación Acme.

- Se desarrolló el instructivo el cual consta de pasos a implementar con la finalidad de poder lograr lo indicado por las normas usadas.

- El uso de la norma ISO 17799:2007 (Código de Buenas Prácticas para la Gestión de la Seguridad de la Información), se vuelve esencial para el análisis de la seguridad física y lógica de la institución.

RECOMENDACIONES

- Corregir las vulnerabilidades mostradas durante el proceso de trabajo, todo esto teniendo como finalidad la seguridad de la información.

- Mantener registros de todos los procesos que se realizan dentro de la Corporación Acme, esto incluye también a las actualizaciones o cambios que se hacen a los diversos aplicativos.

- Establecer un manual, el cual también se tiene que mantener actualizado, esto permitirá mantener a los usuarios bajo un nivel instructivo que disminuiría el riesgo de fallas.

- Asesor y transmitir la cultura sobre los riesgos existentes a nivel de seguridad lógica y física.

- Considerar la Norma ISO 17799:2017 (Código de Buenas Prácticas para la Gestión de la Seguridad de la Información), las cuales ayudarían en el desarrollo de controles y medidas de seguridad.

- Mantener calendarizado los procesos de mantenimientos, ya sea físicos o lógicos, esto permitirá mantener una velocidad de trabajo para los usuarios.

- Corregir todos los puntos relacionados al cableado eléctrico es algo primordial, pues el fluido eléctrico es un recurso importante.

BIBLIOGRAFÍA

Campos, A., Ríos, C. (2016). A*uditoría en el uso de tecnología de información para optimizar la seguridad de la Caja Sipán S.A.* Tesis de Ingeniero en Computación e Informática, Universidad Nacional Pedro Ruiz Gallo, Lambayeque.

Mariñas, G. (2015). A*uditoría informática a la red de datos del Hospital de Tingo María para determinar la situación actual en la que se encuentra y proponer mejoras que garanticen el eficiente funcionamiento de la red corporativa.* Tesis de Ingeniero en Informática y Sistemas, Universidad Nacional Agraria de la Selva, Tingo María.

Monzón, C. (2009). A*uditoria de seguridad de redes inalámbricas de área local Wireless local área Network (WLAN).* Tesis de título de licenciatura en Ingeniería de Sistemas Informáticos, Universidad Mayor de San Andrés, La Paz.

Norma ISO/IEC 17799:2017 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. Presidencia del Consejo de Ministros, Lima, Perú, 16 de enero de 2007.

NIST Special Publication 800-30. National Institute of Standard Technology. Departamento de Comercio, Estados Unidos, 12 se setiembre de 2012.

Rafael, G., Castillo, E. (2017). A*uditoría informática usando las Normas COBITt en el centro de sistemas de información del Hospital Regional Docente Las Mercedes de Chiclayo – 2016.* Tesis de Ingeniero en Computación e Informática, Universidad Nacional Pedro Ruiz Gallo, Lambayeque.

Ramos, C. (2015). *Propuesta de un plan de auditoria informática para el "Sistema de información en salud" y el "Aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015.* Tesis de Ingeniero Informático, Universidad Nacional de Piura, Piura.

Rivera, M., Zambrano, N. (2015). *Auditoria al control y mantenimiento de la infraestructura tecnológica del Departamento Tecnológico de la ESPAM MFL.* Tesis de Título de Ingeniería Informática, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta.

Suárez, S. (2015*). Análisis y diseño de un sistema de gestión de seguridad informática en la empresa Aseguradora Suárez Padilla & CÍA. LTDA., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización*. Tesis de Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia, Bogotá.

Tola, D. (2015). *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la Norma ISO/IEC 27001.* Tesis de Licenciado en Sistemas de Información, Escuela Superior Politécnica del Litoral, Guayaquil.

UNITEL. Normas de Cableado Estructurado [En Línea]. [Consultado 23 de octubre, 2019]. Disponible en Internet: (https://unitel-tc.com/normas-sobre-cableado-estructurado/)

ANEXOS

Anexo 1: Evaluación de la seguridad en la Corporación Acme

Física

Computo

N°	PREGUNTA	SI	NO
1	¿Están los equipos en un lugar adecuado, permitiendo la circulación del personal de forma cómoda?		X
2	¿Existen materiales u objetos que puedan causan aun desastre dentro de la organización, afectando principalmente a los equipos de cómputo?	X	
3	¿Existen grandes presencias de polvo?	X	
4	¿Se cuenta con el espacio suficiente para los Equipos de cómputo?		X
5	¿Es correcta la forma en la que están instalados los equipos de cómputo?		X
6	¿Se tiene lugares diseñados con las características de los diversos equipos?		X
7	¿El piso tiende a generar polvo?		X
8	¿Se cuenta con un área para el mantenimiento de los equipos?		X
9	¿Existe un área determinada, donde se guarden los ordenadores, ya sean en funcionales o no funcionales?		X
10	¿Los equipos están expuestos a ser manipulados por sus usuarios?	X	
11	¿Se cuenta con las herramientas y materiales necesarios para realizar trabajos de mantenimiento y reparación de los equipos de cómputo?		X

Temperatura

N°	PREGUNTA	SI	NO
1	¿La temperatura durante la temporada de verano, es la adecuada para los equipos de cómputo, en todos los ambientes?		X
2	¿Se tiene un controla el nivel de humedad?		X
3	¿El flujo de aire es el adecuado en todos los ambientes?		X

Electricidad

N°	PREGUNTA	SI	NO
1	¿Se cuenta con poso a tierra?	X	
2	¿Existe problemas con las tomas eléctricas?	X	
3	¿Existe problemas con el flujo eléctrico?	X	
4	¿Se cuenta con los planos eléctricos?	X	
5	¿Se cuenta con un sistema de respaldo para la caída de flujo eléctrico?	X	
6	¿Está debidamente separado el flujo eléctrico para los equipos entre las diversas plantas del establecimiento?	X	
7	¿Se cuenta con la señalización reglamentaria en lo que es la caja de llaves eléctricas?	X	
8	¿Existen cables expuestos?	X	
9	¿Las tomas de corrientes se encuentran bien sujetadas, evitando que se suelten al conectar un equipo?		X
10	¿Se usan extensiones o multiplicadores de puertos para conectar diversos equipos?	X	

Seguridad al ingreso y salida

N°	PREGUNTA	SI	NO
1	¿Se cuenta con medidas de seguridad en la Corporación Acme?	X	
2	¿Existe personal responsable de la seguridad?	X	
3	¿El control de seguridad, el cual administra el personal encargado, cubre los equipos de cómputo?		X
4	¿Se realiza la identificación de las personas que salen y entran?	X	
5	¿se realiza algún tipo de chequeo para prevenir la extracción de equipos ajenos a la persona?		X
6	¿En caso se contar con un sistema de cámaras para la vigilancia, el personal de seguridad, tiene control total de estas para monitorear constantemente?		X
7	¿En caso de contar con un sistema de cámaras, este cubre la totalidad de los ambientes dentro del establecimiento?		X
8	¿Existe un control fuera del horario?		X
9	¿Se realizan registros de los usuarios en el sistema para evitar y detectar fallas ocasionados de forma involuntaria o adrede?		X
10	¿Se realizaron registro de entrada y salida en el horario laboral?	X	
11	¿Se controla el uso del personal en equipos de otro usuario?		X

Riesgo de fuego

N°	PREGUNTA	SI	NO
1	¿Cuenta con algún tipo de detección para siniestros involucrados con fuego?	X	
2	¿En caso de contar con algún tipo de detección, estos se encuentran bien distribuidos?		X
3	¿En caso de contar con algún tipo de detección, esta se encuentra funcional en una totalidad del 100%?		X
4	¿Se cuenta con extintores de fuego?	X	
5	¿En caso de contar con extintores de fuego, estos se encuentran distribuidos de la mejor forma?		X
6	¿Existe personal capacitado para el uso de los extintores?	X	
7	¿Se cuenta con salidas de emergencias?		X
8	¿Se cuenta con la señalización necesaria para indicar la salida?		X
9	¿Se cuenta con personal capacitado en caso de incendios?		X
10	¿El control de fechas en los extintores existentes, se realiza?	X	

Seguridad en otros ámbitos

N°	PREGUNTA	SI	NO
1	¿Se controla el préstamo de Equipos o dispositivos?		X
2	¿Existe clasificación de la información?		X
3	¿Se mantiene una copia de las versiones de todos los sistemas, en un determinado lugar?		X
4	¿El guardado de información se realiza de forma automática?		X
5	¿El guardado de información se realiza de forma manual?	X	
6	¿Los cambios realizados en los diversos sistemas, son indicados a los usuarios y a su vez se les hace llegar algún tipo de instructivo?		X
7	¿Existen registros en cada paso del proceso de trabajo?		X
8	¿Existe un encargado en el cuidado y administración, de los backup extraídos de los servidores?	X	
9	¿Todo tipo de modificación es aprobado por algún encargado?	X	
10	¿Existen niveles de acceso a la información para todos los usuarios?		X
11	¿Se lleva un control de errores y fallas?		X
12	¿Se lleva un control de conexión a los equipos, en relación a dispositivos o periféricos?		X

Comunicación

N°	PREGUNTA	SI	NO
1	¿Cuenta con más de un (1) tipo de red?	X	
2	¿Existe un control de antecedentes relacionados a fallas de red?		X
3	¿Se realiza un control del tráfico en la red?		X
4	¿Está registrado la asignación de puertos y números IP?	X	
5	¿Existe algún tipo de respaldo si en caso llegara a caer el enlace de comunicación?		X
6	¿Se cuenta con el plano del cableado de red?		X
7	¿Se realizan pruebas y test para corroborar el buen funcionamiento de la red?		X
8	¿El control de los equipos es realizado por un personal capacitado?		X
9	¿Existe algún tipo de protección para los principales cables de conexión expuesto al clima externo?		X

10. ¿Cuál es la tecnología usada para la conexión dentro de la Corporación Acme?

    TCP/IP

11. ¿Qué tipo de topología se usa?

    Estrella

12. ¿Qué categoría de red se trabaja?

    Categoría 6

Anexo 2: Preguntas para las entrevistas

1. ¿Cuál es el principal recurso de la Corporación Acme?
2. ¿Cuál sería la principal amenaza contra el recuso identificado en la anterior pregunta?
3. ¿Cree poder indicar el cómo se podría reducir el riesgo de amenaza para el principal recurso nombrado? Breve explicación
4. ¿Qué otros recursos considerarían prioritarios para ser protegidos?
5. ¿Conoce alguna medida ya tomada para contrarrestar las amenazas emergentes?
6. ¿El equipo con el que trabaja durante su jornada laboral, presenta algún problema? Indicar
7. ¿Encuentra usted alguna falla en el método de trabajo para el cuidado de la información?
8. ¿Podría mencionar la última vez que se le realizaron mantenimiento a los equipos?
9. ¿Siente que existen niveles de seguridad tanto para el personal, como para los diversos sistemas?

Anexo 3: Cuestionarios internos

Evaluado: Corporación Acme			
Evaluador:			
Fecha:			
Proceso: Seguridad física			
Objetivo: Verificar la seguridad física dentro de la Corporación Acme			
Preguntas	**Si**	**No**	**Observación**
¿Cuenta con un control de acceso?	X		Huella dactilar
¿Se controla la salida durante la jornada laboral?	X		Boletas con firma y sello, del superior a cargo
¿Se lleva un control de los equipos que salen y entran?		X	
¿Se cuenta con un control de acceso al espacio asignado para los equipos de comunicación?		X	
¿Durante la presencia de algún visitante, se le hace algún tipo de control durante su estadía en las instalaciones?		X	
¿Al concluir la visita, se le hace algún tipo de chequeo?		X	
¿Se lleva un monitoreo mediante las cámaras?	X		
¿El monitoreo se lleva también fuera del horario laboral?		X	
¿Se realizan evaluaciones para determinar el nivel de funcionamiento de los equipos?		X	
¿Existen procesos que ayuden al funcionamiento de los servidores?	X		Reinicio programado durante el fin de semana
¿Existen procesos que ayuden al funcionamiento de los equipos usados por el personal?		X	
¿Se realiza un control de estado físico, para todos los equipos informáticos?		X	
¿Se cuenta con personal capacitado para el mantenimiento de todos los equipos?		X	

Evaluado: Corporación Acme			
Evaluador:			
Fecha:			
Proceso: Seguridad lógica			
Objetivo: Verificar la seguridad lógica dentro de la Corporación Acme			
Preguntas	**Si**	**No**	**Observación**
¿Se cuenta con algún control de acceso?		X	
¿Todo el personal dentro de la Corporación Acme, tiene conocimiento de sus limitaciones al acceder a información?		X	
¿Se cuenta con niveles de confiabilidad en lo que son los password de acceso?		X	
¿Existen controles para evitar softwares maliciosos?	X		Antivirus
¿Existen accesos limitados por la designación de ip?	X		Principalmente para la navegación web
¿La configuración de red, abarca todos los equipos dentro?		X	
¿Se cuenta con control y registro de actualizaciones?		X	
¿Se llevan registros de fallas por parte de los aplicativos?		X	
¿Se llevan Registro de soluciones a las fallas presentadas por los aplicativos		X	
¿Se lleva un control de las licencias?		X	
¿Existen procesos para mejorar el rendimiento de los aplicativos?		X	

Anexo 4: Formulario de visitas

Formulario
Especificación: Área de Sistemas
Lugar: Corporación Acme
Fecha:
Observaciones
- El espacio asignado para realizar trabajos es limitado. - Carencia de herramientas suficientes. - No todo el personal está capacitado en diversas funciones. - El área de sistemas esta dividido en 2: Desarrollo y Soporte. - No se cuenta con un registro de acciones realizadas.
Encargado:

Formulario
Especificación: Cableado de Red
Lugar: Corporación Acme
Fecha:
Observaciones
- Puntos de red no están identificados. - Puntos en el patch panel no se encuentran trabajando. - Cableado y equipos colocados de forma provisional.
Encargado:

Formulario
Especificación: Data Center
Lugar: Corporación Acme
Fecha:
Observaciones
- El manejo y orden del cableado estructurado no es el correcto. - Patch cord no conectados y con un tamaño no apropiado. - No están etiquetados los equipos y cables para su comunicación. - Equipos expuestos y con falta de mantenimientos.
Encargado:

Formulario
Especificación: Red Eléctrica
Lugar: Corporación Acme
Fecha:
Observaciones
- Tomas mal fijadas en la pared. - Cableado expuesto. - Puntos eléctricos no funcionales. - Uso exagerado de extensiones debido a la carencia de puntos eléctricos bien ubicados
Encargado:

Formulario
Especificación: Ordenadores (Computadoras)
Lugar: Corporación Acme
Fecha:
Observaciones
- Equipos presentan falta de mantenimiento lógico. - No todos cuentan con un uso compartido de información. - No cuentan con mantenimiento preventivo según calendario. - No se etiqueta el inventario originando confusiones al desplazarlos de un lugar a otro. - Algunos se encuentran expuestos a ser golpeados. - Si sucediera algún derramamiento de liquido en el suelo, muchos se verían comprometidos. - Periféricos de trabajo como el teclado presentan rigidez.
Encargado: