RESUMEN – TRABAJO DE GRADO

AUTORES	**JOSE LUIS QUINTERO GARCÍA** **JOSE LUIS MARTÍNEZ MENDOZA**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION AUDITORIA DE SISTEMAS**
DIRECTOR	**ANDRES MAURICIO PUENTES**
TÍTULO DE LA TESIS	**PLANTEAMIENTO DE UNA GUÍA PARA EL MEJORAMIENTO DE LA SEGURIDAD FÍSICA DE LA EMPRESA TMSOFT S.A.S**

RESUMEN

(70 palabras aproximadamente)

DURANTE EL DESARROLLO DE LA AUDITORIA SE PUDO CONSTATAR QUE LA EMPRESA CARECE DE MANERA GENERAL DE PLANES DE CONTINGENCIA EN CASO DE EMERGENCIA, ADEMÁS DE CARECER DE CONTROLES QUE PERMITAN CONTROLAR EL ACCESO A LAS ÁREAS CRÍTICAS DE LA EMPRESA PONIENDO EN RIESGO TANTO LOS ACTIVOS FÍSICOS DE LA EMPRESA COMO LA FIABILIDAD E INTEGRIDAD DE LA INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 76	PLANOS:	ILUSTRACIONES:	CD-ROM:

PLANTEAMIENTO DE UNA GUÍA PARA EL MEJORAMIENTO DE LA SEGURIDAD FÍSICA DE LA EMPRESA TMSOFT S.A.S

Autores:

JOSE LUIS QUINTERO GARCÍA

JOSE LUIS MARTÍNEZ MENDOZA

DIRECTOR

ANDRES MAURICIO PUENTES

INGENIERO DE SISTEMAS

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACION AUDITORIA DE SISTEMAS

Ocaña, Colombia Octubre de 2017.

Índice

Pág.

Lista de figuras

Lista de tablas

pág.

Introducción

Los recursos tecnológicos son importantes para vida de los individuos y en especial para el buen funcionamiento de una organización. Ellos facilitan la transmisión de datos, el acceso a información y su almacenamiento, convirtiéndolos en un bien de vital importancia para toda organización. En la actualidad, las herramientas tecnológicas han servido para optimizar y mejorar ámbitos como la educación, proyectos humanitarios, la inteligencia colectiva o la gestión de ideas creativas, gestión de personal en las empresas, en fin, un sin número de beneficios donde su mayor aporte es abaratar costes, tiempo y esfuerzo, y lograr que tareas básicas sean más eficientes y rápidas.

Por su parte la información -que es un recurso necesario e importante generado gracias a sistemas de información y el uso del recurso tecnológico para facilidad de su almacenamiento y disposición- es una parte vital de toda organización, y es ésta, la que suministra un alto nivel de competitividad frente a la competencia.

Estos dos recursos (tecnología, información) contribuyen a la administración, gerencia y buen funcionamiento de las empresas, es por ello recomendable, dotar a la organización de medios que garanticen la seguridad de estos recursos.

TMSOFT S.A.S. es una organización de carácter privado, de base tecnológica, que ofrece servicios de Networking, Consulting y Auditoría en telecomunicaciones, Desarrollo de software, alquiler de servidores dedicados y planes de soporte. A esta empresa hemos hecho una valoración donde tenemos en cuenta las medidas técnicas organizativas y legales que permiten a la organización asegurar la confidencialidad, la integridad y disponibilidad de estos recursos. Por tanto, nos encontramos con una serie de oportunidades de mejora, las cuales no lleva a

desarrollar una guía para el mejoramiento de la seguridad física y ambiental de ésta organización y mitigar los daños y ataques que pueda sufrir.

Capítulo 1. Planteamiento de una guía para el mejoramiento de la seguridad física y ambiental de la empresa TMSOFT S.A.S.

1.1 Planteamiento del Problema

La seguridad y la violencia son los temas que más preocupan a los colombianos. Gran parte del pueblo pone ésta problemática por encima de temas cómo el desempleo, fallas de seguridad social y el acceso a la educación, estos temores son trasladados también a las empresas.

Muchas empresas en Colombia desconocen lo básico en temas de seguridad de la información, donde ellas, no pueden visualizar un ataque o intromisión a sus sistemas como tampoco las deficiencias que estructuralmente posee para salvaguardar sus equipos y la información contenida en ellos.

La empresa TMSOFT S.A.S, adolece de una guía que permita llevar acabo el mejoramiento de la seguridad física, la cual, debe estar diseñada para su entorno en particular que facilite la alineación de los objetivos de la empresa. Ésta situación conlleva a que en los últimos años se haya invertido muchos recursos (dinero, tiempo, personas) en la adecuación o adquisición de tecnología e infraestructura, sin una planeación adecuada, sin un análisis previo de las necesidades de la organización, ocasionando que la inversión se pierda, y que no se obtengan los resultados esperados.

La empresa TMSOFT S.A.S. es una organización de carácter privado, de base tecnológica, que ofrece los servicios de Networking, Consulting y Auditoría en telecomunicaciones, Desarrollo de software, alquiler de servidores dedicados y planes de soporte. Esta empresa del sector de las comunicaciones que ofrece productos y servicios tecnológicos presenta la necesidad de contar con una guía que permita mejorar la seguridad física y que contribuya a la consecución de los objetivos del negocio apoyados eficientemente en la tecnología.

Ante los problemas de seguridad y la ausencia de garantías de protección por parte de las entidades del estado, el presente trabajo pretende plantear una guía que permita llevar a cabo el mejoramiento de la seguridad física de la empresa TMSOFT S.A.S. Teniendo en cuenta la importancia que tiene la información para una organización, tomamos como referente la definición que da la norma ISO 27001 "La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente" con lo cual, tomamos la importancia de la información y los recursos tecnológicos como un activo primordial de la empresa y la necesidad de salvaguardar éste recurso.

1.2 Formulación del Problema

¿Puede una guía para la implementar el dominio seguridad física y ambiental de la NTC/ISO 27001; 2013 contribuir con prevención del acceso físico no autorizado, daño e interferencia con la información y las áreas de la empresa TMSOT S.A.S?

1.3 Objetivos

1.3.1 Objetivo General

Diseñar una guía para la implementación del dominio seguridad física y ambiental de la NTC/ISO 27001:2013 en la empresa TMSOFT S.A.S.

1.3.2 Objetivos Específicos

- Realizar una auditoría que permita identificar hallazgos asociados a la seguridad física y ambiental en la empresa TMSOFT S.A.S.

- Diagnosticar los riesgos y situaciones que actualmente presenta la empresa TMSOFT S.A.S en su estructura física y ambiental.

- Establecer las respectivas recomendaciones para garantizar la seguridad física y ambiental de la empresa TMSOFT S.A.S.

1.4 Justificación

La razón principal para crear una guía que optimice la seguridad física y ambiental de la empresa TMSOFT S.A.S es la necesidad que surge, debido a la detección de un sin número de irregularidades detectadas por observación, al momento de realizar una visita programada a la empresa, con la cual, buscamos medir las necesidades presentadas en ella.

La empresa y su recurso humano se verían beneficiadas debido a que se garantiza la disponibilidad y continuidad de los equipos de cómputo, el tiempo que requieran los usuarios para el procesamiento oportuno de las aplicaciones, comprobar que los planes y políticas de seguridad y de recuperación sean conocidos y difundidos por la gerencia, constatar que se brinde la seguridad necesaria a los diferentes equipos de cómputo que existen en la empresa TMSOFT S.A.S y controles necesarios para seguridad en el área (inventario de equipos, resguardo de equipos, bitácoras de mantenimiento y correcciones, controles de perímetro para restringir el acceso del personal a las áreas críticas).

1.5 Hipótesis

El diseño de una guía está orientado a fortalecer la seguridad que llevará a la empresa TMSOFT S.A.S a garantizar la disponibilidad, integridad y confidencialidad de la información propia y de sus clientes consolidándose con una entidad que garantiza la seguridad de los datos.

1.6 Delimitaciones

1.6.1 Delimitación Temporal. El desarrollo del presente proyecto tendrá una duración de 3 meses contados a partir de 7 de enero de 2017 veintiún días después de la finalización de las actividades académicas del curso de auditoria de sistemas.

1.6.2 Delimitación Geográfica. El lugar donde se aplicará el presente proyecto es la empresa TMSOFT SAS en la ciudad de Ocaña.

1.6.3 **Delimitación Contextual.** El proyecto se desarrollará dentro de las instalaciones de la empresa TM SOFT S.A.S a todos sus empleados y directivos.

1.6.3.1 Reseña Histórica de Ocaña. Ocaña está situada a 8º 14' 15" Latitud Norte y 73º 2' 26" Longitud Oeste y su altura sobre el nivel del mar es de 1.202 m. La superficie del municipio es 460Km², los cuales representan el 2,2% del departamento. La Provincia de Ocaña tiene un área de 8.602 km². Posee una altura máxima de 2.065 m sobre el nivel del mar y una mínima de 761 m sobre el nivel del mar. Es la segunda ciudad después de Cúcuta del departamento de Norte de Santander.

Entre el grupo de heroicos guerreros que por orden del gobernador de Santa Marta Don Pedro Fernández del Bustos, partieron de esa ciudad, en los primeros días del mes de abril de 1570 para explorar las cabeceras del Río Magdalena, era conocido el nombre del capitán Francisco Fernández de Contreras. Fue pues, sin duda alguna, el fundador de Ocaña uno de los compañeros de aquel que respondía al nombre de Gonzalo Jiménez de Quesada. Su espada adiestrada en mil combates luchó por la reducción de los Chibchas y con incalculables y temerarias hazañas estampó su nombre glorioso entre el cuadro glorioso de los fundadores de la ciudad de Santa Fe en tanto que su vigorosa juventud paladeaba el triunfo. Más tarde, al lado de Don Ortún Velasco de Velásquez y de Don Pedro de Orsúa, aparece Fernández de Contreras, también de la legendaria e histórica ciudad de Pamplona. Su reconocido valor bien, pronto lo acreditó entre sus compañeros y, entonces, se le nombra jefe de la expedición que vino a culminar con el glorioso establecimiento de Ocaña. Ocaña fue fundada el l4 de diciembre de 1570.

Sucedió pues, que el día 26 de julio de 1570, el capitán Francisco Fernández de Contreras, seguido de sus tenientes y soldados, entre los cuales que se distinguían Juan Lorenzo, Diego Páez de Sotomayor, Gaspar Barbosa de María y otros más que junto a él y bajo las ordenes de Don Pedro de Ursua, habían conquistado y fundado Pamplona. En nombre de la majestad de Don

Felipe II tomó posesión de las tierras de Hacaritama, cuyos habitantes avisados de la cercanía de los españoles, presentándose en paz y no poco sorprendidos del ceremonial y la pompa guerrera con la que el capitán había querido rodear la fundación de la nueva ciudad. En el año 1573, ya por los continuos ataques indígenas, ya por el deseo de aproximar (4 kilómetros) un poco la ciudad al puerto (Gamarra), o posiblemente por las inundaciones que, en épocas de invierno sufrían aquellas tierras, se efectuó el traslado de Ocaña al sitio que actualmente ocupa, y desde entonces aquellos valles bañados por el río Algodonal o Catatumbo, fueron bautizados como " Llano de los Alcaldes". Además de ostentar desde el año de 1575 el título de ciudad, conferido por Real Cédula del soberano de España; de figurar como capital de cantón primero y después de la provincia de su mismo nombre, con asiento del Gobernador de Seccional y de la Cámara Legislativa al decretarse por el congreso de 1849 una nueva división territorial, Ocaña fue una de las primeras ciudades que le cupo en suerte recibir al Libertador Simón Bolívar (1813), cuando se iniciaban en la Nueva Granada las campañas libertadoras; ocupa igualmente sitio preferente por haber sido Capital de la República (15 de abril de 1824) y por ser escogida para la reunión de la Gran Convención en 1828.1

1.6.3.2 Reseña Histórica TMSOFT S.A.S. Es una empresa fundada en 2009 por los ingenieros Alberto Cabrales Y Alexander cruz con la idea de la integración de productos y servicios tecnológicos y de telecomunicaciones para las empresas. Diseñando desarrollando e integrando productos propios con productos de reconocidos fabricantes, lograron posicionar sus soluciones enfocadas en la eficiencia y el aumento de la productividad en importantes empresas de diversos sectores tanto en nuestro país como en el exterior.

En el 2015 fue reconocida por el ministerio de las TIC de Colombia y el ministerio de comercio exterior como marca Colombia, empresa embajadora del país en el exterior.

Capítulo 2. Marco referencial

2.1 Marco Histórico

La empresa TMSOFT S.A.S no cuenta, ni ha implementado un diseño de una guía para el mejoramiento de la seguridad física de la empresa.

A continuación, se hará referencia de algunas investigaciones:

- METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS APLICADOS A LA SEGURIDAD INFORMÁTICA Y DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27001. Francisco Nicolás Javier Solarte Solarte1, Edgar Rodrigo Enríquez Rosero2, Mirian del Carmen Benavides Ruano3.

El artículo tiene como objetivo desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Se presentan los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, clave de seguridad, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que permitieron establecer el diagnóstico de seguridad actual.

- PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN ÁREA CONTABLE EN LA EMPRESA TRANSFORMADORES CDM. Joaquin Guerrero Melo, Francisco Javier Suarez Castrellon

“El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados” Gene Spafford, con esta frase debemos reconocer que la información no está 100 % protegida pero si podremos minimizar el riesgo para que no sea objeto de ataques cibernético, robos de información y virus informáticos. Es por eso que en este proyecto de planeación del sistema de seguridad de la información, la norma internacional ISO/TEC 27001 fue aplicada en área contable en la empresa TRANSFORMADORES CDM para la protección de la información de esta área específica y poder realizar protocolos para no caer en los problemas e informar a los usuarios lo que deben saber para no caer fácilmente en ataques externos o virus informáticos y posible pérdida de información.

- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA GENERAL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA DE ACUERDO A LA NORMA ISO/IEC 27001:2013. Álvaro Javier Durán Sanjuán Jorge Luis Peinado Rodríguez.

En definitiva, la información es el activo más valioso de cualquier organización, debido a esto, protegerla debe ser un objetivo claramente establecido. La necesidad de garantizar por lo menos la integridad, confidencialidad y disponibilidad de la información, ha conllevado a las organizaciones a ocuparse de lo que actualmente se conoce como sistema de gestión de la seguridad de la información (SGSI), apoyado por la trascendencia que han tomado las normas internacionales y las buenas prácticas para la gestión de dicho activo. Con miras a establecer el SGSI, organizaciones de todos los tipos han iniciado el proceso con la definición de políticas de seguridad de la información, de modo que son una herramienta organizacional que busca

contribuir a la sensibilización del talento humano en cuanto a la importancia y criticidad de la información.

2.2 Marco Teórico

Esta Investigación abarca diferentes teorías, que son de vital importancia para el entendimiento y la realización del mismo, entre éstas se puede mencionar:

2.3 Marco Legal

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

La misma ley en su **artículo 269A**. Hace referencia al acceso abusivo a un sistema informático. Toda persona que logre entrar a un sistema informático que esté protegido o que tenga una medida de seguridad, sin ningún permiso de aquel que tenga el legítimo derecho, para robar o alterar la información incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

En este orden de ideas la citada normal en su **artículo 269c** se refiere a la interceptación de datos informáticos manifestando que el que, intercepte datos informáticos sin ninguna orden judicial con un sistema informático que los transporte, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

En relación con los daños informáticos, el **artículo 269D** estipula el que, sin ningún derecho este facultado para destruir, dañe, borre, deteriore, altere o suprima datos informáticos de un sistema de información incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Sobre el uso del software malicioso el **artículo 269E** de la susodicha ley expresa el que, sin estar facultado para producir, traficar, adquiera, distribuya, venda o envié, software malicioso o dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes; así mismo el **Articulo 269** trata sobre la violación de datos personales manifiesta que la persona que no esté facultado en complicidad de un tercero obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.4 Marco Conceptual

ISO 27001. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (Academy 27001, 2013).

Seguridad física. Dentro de la seguridad informática, la seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. La seguridad física se complementa con la seguridad lógica. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son:

- Desastres naturales, incendios accidentales, humedad e inundaciones.
- Amenazas ocasionadas involuntariamente por personas.
- Acciones hostiles deliberadas como robo, fraude o sabotaje. (Alegsa, 2010)

Control de acceso. Es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de próximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor. (Villegas, 2009)

Vulnerabilidad. Es la incapacidad de resistencia cuando se presenta un fenómeno amenazante o para reponerse después de que ha ocurrido un desastre, es el factor complejo de riesgo o el grado de exposición a sufrir algún daño por la manifestación de una amenaza específica. (Ortega Ruiz, 2014).

Riesgos. En arquitectura de computadores, un riesgo es un problema potencial que puede ocurrir en un procesador segmentado. Típicamente los riesgos se clasifican en tres tipos: riesgos de datos, riesgos de salto o de control y riesgos estructurales.

Las instrucciones de un procesador segmentado son ejecutadas en varias etapas, de modo que en un momento dado se encuentran en proceso varias instrucciones, y puede que éstas no

sean completadas en el orden deseado. Un riesgo aparece cuando dos o más de estas instrucciones simultáneas (posiblemente fuera de orden) entran en conflicto. (Vera Cortes, 2016).

Servidor. Es la máquina informática u ordenador que está al servicio de otras máquinas u ordenadores, llamadas clientes. La finalidad de un servidor es suministrar la información o proveer datos que solicitan los clientes y, para ello existen diferentes tipos de servidores, como por ejemplo:

- **Servidor Web,** almacena y envía a los clientes documentos en HTML, imágenes, videos, textos, etc.

- **Servidor de correo**, como lo indica su nombre se encarga de almacenar, enviar, recibir y realizar todas las operaciones ligadas al correo electrónico

- **Servidor de impresión:** Se encarga de administrar los diferentes documentos que se envían para imprimir dentro de la red

- **Servidor de base de datos: E**s un sistema que permite almacenar grandes cantidades de información y el servidor permite almacenar y gestionar o administrar bases de datos

- **Servidor de archivos:** hace referencia al uso del disco duro compartido por varios usuarios y que sea usado por un único usuario, por ejemplo: cuando varios usuarios intentan acceder a una misma información, el servidor de archivos controla y ordena los accesos a esta, permitiendo el ingreso de un número de usuarios y a la vez otros se encuentran en espera.

- **Servidor proxy:** este trabaja como un intermediario entre 2 ordenadores, en ocasiones este servidor puede bloquear ciertas peticiones que realiza el cliente debido a que posee ciertas extensiones bloqueadas y por lo tanto, no se puede acceder a la página solicitada por el cliente.

- **Servidor DNS:** Son las siglas de (Domain Name System), se asocia una información con un nombre de dominio y este servidor determina en qué lugar se encuentra esa página web y nos remite a ella, tal como fue solicitada por el cliente. (Fernández, 2015)

2.5 Marco Contextual

El proyecto se realizará en la empresa TMSOFT S.A.S localizada en la CALLE 10 # 15-51 en el barrio san Agustín en Ocaña, NORTE DE SANTADER, la cual presta servicios de telefonía IP y asesoría en la configuración de redes.

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

El tipo de investigación para el desarrollo del proyecto será La investigación descriptiva, tiene como objetivo identificar los riesgos potenciales y las vulnerabilidades a las cuales están expuestas las operaciones de la empresa y analizar el impacto en ella, el estado, las características, factores y procedimientos presentes en fenómenos y hechos que ocurren (Lerma Gonzales, 2009).

Inicialmente se realizará un análisis de la problemática que se presenta en la empresa TMSOFT S.A.S, debido a la ausencia de políticas de seguridad de la información ya que la información se encuentra expuesta a vulnerabilidades como uso de contraseñas débiles, configuración de acceso a recursos sin contraseña, uso de cuentas Invitado, ataques o robos, entre otros que podrían llevar a la empresa a tener grandes pérdidas. De esta manera se hace una breve descripción del problema a resolver, donde se encontrarán las variables a tener en cuenta para el desarrollo de este proyecto y la puesta en marcha del mismo.

3.2 Población y muestra

Para determinar la población objeto de estudio del proyecto se determina al personal administrativo como el foco de interés, conformado por el contador, secretaria general y gerente y a los ingenieros del área de desarrollo y a los técnicos de instalación. Al ser una población finita y medible, se decide elegir como muestra para el presente estudio al 100% de la misma.

3.3 Técnicas e instrumentos de recolección de información

Las técnicas de recolección de datos que serán aplicadas en este proyecto son: la observación directa y entrevista estructurada. Mediante el análisis y la observación se obtendrá información sobre lo que ocurre en la empresa en el manejo de la información y la seguridad de la misma, se tomaran datos sobre los problemas e inquietudes que presentan tanto el personal administrativo como técnicos e ingenieros; en relación con la técnica de la entrevista; se realizara

directamente en el área administrativa y a los técnicos e ingenieros donde se recogerá gran cantidad de información, se desarrollaron una serie de pregunta al personal donde se obtendrá información importante para el avance del proyecto.

3.4 Análisis de información

Luego de realizarse la entrevista se hará un análisis detallado de los datos recolectados con el fin de identificar de manera clara y precisa las falencias de la empresa TMSOFT S.A.S en el área de seguridad física y ambiental, estas falencias servirán de base para el planteamiento de la guía que permita dar solución a las mismas.

La construcción de la guía se realizara teniendo en cuenta los hallazgos encontrados luego de la ejecución de las diferentes herramientas plateadas anterior mente, usando como guía la norma ISO 27001 para el planteamiento de las diferentes recomendaciones.

Capítulo 4. Presentación de resultados

Proteger los equipos de cómputo y la información contenida en ellos, es uno de los aspectos más importantes de salva guardar de una empresa u organización. Estos bienes cuya representación se manifiesta en dinero, necesitan de una metodología que permita evaluar los controles e infraestructura de una empresa, con el fin actuar de la manera necesaria y mitigar los riesgos a los que se exponen tan solo por el hecho de existir.

Toda empresa necesita de una metodología que estandarice los controles y acciones necesarios para disminuir el riesgo de pérdida de información, daños en equipos e integridad del elemento humano de una empresa.

Tomando como referencia el cuadro de actividades trazados desde el principio del desarrollo de nuestro proyecto de grado, se ha cumplido con todas las actividades programadas.

4.1 Auditoria a la seguridad física y ambiental a la empresa TMSOFT S.A.S

Teniendo en cuenta los hallazgos obtenidos en cada una de nuestras visitas a la empresa TMSOFT S.A.S. se han encontrado una serie de anomalías concentradas sobre todo a nivel físico y estructural de la empresa.

Las instalaciones no cuentan con las medidas físicas que garanticen la seguridad e integridad de los equipos, ya sea, por intervención del hombre o de los diferentes aspectos ambientales que se dan en el medio.

Objetivo de la auditoria. Evaluar los controles, sistemas, procedimientos y funcionamiento de la empresa TMSOFT S.A.S, para identificar los factores que afecten la integridad de la seguridad física y ambiental de la empresa.

Alcance de la auditoria. Revisar todos los procedimientos establecidos en la empresa TMSOFT S.A.S verificando la existencia de controles que garanticen la seguridad física y ambiental de la empresa y el cumplimiento de los mismos.

Metodología empleada. La presente auditoría pretende recolectar y evaluar las evidencias para determinar si dentro de la empresa TMSOFT S.A.S, se cuenta con los requerimientos mínimos contemplados en los objetivos de control de seguridad física y ambiental de la norma NTC/ISO 27001; 2013, para tal efecto se hace uso de una metodología cuantitativa con un enfoque descriptivo.

La población a estudiar está constituida por el personal del Área de Sistemas de la empresa TMSOFT S.A.S., y la muestra corresponde al 100% de la población, debido a que el número de personas es fácilmente manejable (cuatro personas).

Se desarrollaron encuestas y cuestionarios como método de recolección de información, las cuales fueron aplicadas al Área de Sistemas de la empresa TMSOFT S.A.S. (Ver anexo B y anexo C).

4.1.2 Ejecución de pruebas

Para evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización, se crean áreas seguras donde se definen:

1. Perímetros de la seguridad física
2. Controles físicos de entrada
3. Seguridad de oficinas, despachos y recursos
4. Seguridad contra amenazas externas y del entorno

Estas pautas son necesarias para aplicar seguridad física y modelos de trabajo en las áreas seguras.

Tomando ésta serie de conceptos elaboramos los formatos con las situaciones encontradas en la empresa TMSOFT S.A.S.

FORMATO DE SITUACIONES ENCONTRADAS AC-14			**EMPRESA:** TMSOFT S.A.S		
FECHA DE ELABORACION: 26 de Diciembre de 2016					
AREA AUDITADA: Sistemas Desarrollo y Soporte					
REF.	**Situación**	**Causas**	**Solución**	**Fecha de Solución**	**Responsable**
SE.1	No existe protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables	No se ha realizado los planes de contingencia en caso de emrgencias	Implementar un sistema de protección y un plan de contingencias frente a los factores meteorológicos que se puedan presentar en un futuro	20 de Enero DE 2017	Equipo de recurso humano
SE.2	No se encontraron extintores cerca de los equipos lo que implica unos riegos inminentes de perdida de información y equipos en caso de incendio.	Falta de importancia por parte de los representantes de la empresa en el adecuamiento de las instalaciones fisicas con sus respectivos articulos.	Elaborar el sistema en seguridad y salud en el trabajo que se debe desarrollar para todas las empresas por ley, basaso en el decreto 1072 de 2015	20 de Enero de 2017	Implementar una alarma contra incendios complementado con extintores de tipo Novec 1230 o FM200 / FE-13
SE.3	No existe un manual definido y socializado de las actividades y funciones que cumplen cada uno de los empleados.	No existencia de organización en el establecimiento de documentos que enmarquen las actividades	Crean un manual de funciones y procedimeinto, asi mismo socializarlo y darlo a conocer a todos los empleados del area.	20 de Enero de 2017	Equipo de recurso Humano
SE.4	Los equipos no tienen un sistema de refrigeración o ventilación adecuado haciendo evidente las altas temperaturas en el área ya mencionada	El espacio en el cual se encuentran los servidores y otros equipos no es adecuada y no cumple con las condiciones mínimas para el correcto funcionamiento de los mismos	Instalar un sistema de aire acondicionado que permita mantener la refrigerado el cuarto -Instalar medidores de temperatura y humedad	20 de Enero de 2017	Ordenador del gasto y jefe de la empresa

FORMATO DE SITUACIONES ENCONTRADAS AC-14	EMPRESA: TMSOFT S.A.S
FECHA DE ELABORACION: 26 de Diciembre de 2016	
AREA AUDITADA: Sistemas Desarrollo y Soporte	

REF.	Situación	Causas	Solución	Fecha de Solución	Responsable
SE.5	La ubicación de los equipos no es la adecuada ya que no cuenta con un acceso controlado y registrado.	Porque el espacio de la empresa es muy pequeño y no cuenta con lugares mas comodos y seguros para los equipos	Instalar una cerradura electrónica que permita llevar el registro de los empleados que acceden al cuarto de servidores	20 de enero de 2017	Jefe de la empresa
SE.6	Los cambios de contraseñas aunque son notificados vía correo, no cuentan con un respaldo de quien los realizó.	No existe organización por parte del personal	Realizar ataques de seguridad constantes provocados por la empresa para chequear constancia y robustez en los servidores que contienen la información.- Desarrollar e implementar un sistema de seguridad confiable para el mantenimiento de las contraseñas de seguridad.	20 de enero de 2017	Equipo operativo del area de sistemas
SE.7	Se evidenció que en caso de ocurrir un corte de energía inesperado los equipos del personal de desarrollo no cuentan con un sistema de emergencia que pueda permitir el almacenamiento confiable de los procesos desarrollados hasta ese momento.	No se cuenta con manuales documentados en caso de emrgencias	Instalar UPS (Uninterruptible Power Supply) fuente de poder interrumpible que permita el almacenamiento de la información manipulada y desarrollada en los diferentes equipos que lo requieran.	23 de Marzo de 2017	Equipo operativo del area de sistemas

FORMATO DE SITUACIONES ENCONTRADAS AC-14			EMPRESA: TMSOFT S.A.S		
FECHA DE ELABORACION: 26 de Diciembre de 2016					
AREA AUDITADA: Sistemas Desarrollo y Soporte					
REF.	**Situación**	**Causas**	**Solución**	**Fecha de Solución**	**Responsable**
SE.8	El área de sistemas no cuenta con un inventario de software	No se ha realizado por falta de interés del personal del área	Generar un inventario de software que permita establecer con que herramientas cuenta la empresa.	23 de Marzo de 2017	Jefe del area de sistemas y equipo operativo
SE.9	No se encontró un mecanismo de control que regule la descargar de software potencial mente peligroso	Falta de tiempo y compromiso	Docuemntar mecanismos de regulacion al descargar informacion que deba ser ingresada e indezada en el sistema	26 de Marzo de 2017	Jefe del area de sistemas y equipo operativo

Figura 1. Formato de situaciones encontradas

Fuente. Los Autores

Formatos con las desviaciones detectadas en la empresa TMSOFT S.A.S.

RESUMEN DE DESVIASIONES DETECTADAS AC-12			EMPRESA: TMSOFT S.A.S
FECHA DE ELABORACION: 19 de Diciembre de 2016			
AREA AUDITADA: Sistemas Desarrollo y Soporte			
Ref.	**Situaciones**	**Causas**	**Solución**
DDT.1	Mecanismos que garanticen la seguridad física de los equipos.	Robo, fraude y mal uso de las instalaciones y medios.	Que se documenten y establezcan revisar los mecanismos por medio de los cuales el sitio genere las medidas necesarias para garantizar la seguridad de los equipos.
DDT.2	Condiciones no aceptables en las que se encuentren las servidores	Por falta de conocimiento y mantenimiento, generados por falta de revision y cuidado del personal a cargo.	Implementación de estrategias que minimicen el inpacto que se genera al no tener los servidores en condiciones adecuadas.
DDT.3	factores ambientales y prevencion de riesgo	No existe protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos o desastres naturales incontrolables y accidentes.	Implementar un sistema de protección y un plan de contingencias frente a los riesgos y amenazas que se puedan presentar.

Figura 2. Formato de resumen de las desviaciones detectadas

Fuente. Los Autores

4.2 Identificación de riesgos

Para la identificación de riesgos se tuvo en cuenta las respuestas que fueron formuladas en la empresa TMSOFT S.A.S., y cuyos cuestionarios fueron descritos anteriormente.

Para la asignación de la probabilidad y el impacto en cada uno de los riesgos se utilizaron las siguientes escalas:

Tabla 1. Probabilidad

Muy probable	0.9
Bastante probable	0.7
Probable	0.5
Poco probable	0.3
Improbable	0.1

Fuente. Módulo de Auditoría al Desarrollo de Proyectos de Ingeniería

Nota: La siguiente tabla muestra los niveles de probabilidad de ocurrencia, con su respectivo valor.

Tabla 2. Impacto

Muy alto	0.8
Alto	0.4
Moderado	0.2
Bajo	0.1
Muy bajo	0.05

Fuente. Módulo de Auditoría al Desarrollo de Proyectos de Ingeniería

Nota: La siguiente tabla muestra los niveles de impactos que genera, con su respectivo valor.

4.2.1 Análisis cuantitativo de los riesgos
- Riesgos

RT = Riesgo técnico

RE = Riesgo externo

Codigo	Causa	Descripcion del Riesgo	Referencia	Relacion	Probabilidad (p)	Impacto (I)	PXI
RT001	Politicas	Debido a la falta de politicas que permitan llevar acabo acciones efectivas en caso de incendio evitando el daño de los equipos y la perdida de la informacion.			0,1	0,01	0,01
RE002	Politicas - Controles	No existen politicas ni controles claros que regulen y registren el acceso del personal al datacenter de la empresa.			0,7	0,8	0,56
RE003	Controles - Documentacion	Al carecer controles de acceso a las instalaciones se pone en riesgo la integridad de los equipos de la empresa.			0,5	0,8	0,4
RT004	Controles	Por no contar con el respaldo adecuado un fallo electrico puede afectar a los equipos.			0,1	0,1	0,01
RT005	Calidad - Planificacion	No contar con planes de contingencia adecuados se puede ver afectada la continuidad del negocio impactando directamente en el servicio a los clientes.			0,5	0,2	0,1

Figura 3. Análisis Cuantitativo de los riesgos

Fuente. Los Autores

Planificación de la respuesta a los riesgos del proyecto

RT = Riesgo técnico

RE = Riesgo externo

Codigo	Estreategia y Acciones	Contingencias y Respaldos	Responsable	Fecha
RT001	Mitigar	Crear un plan de atencion a emergencias	Area de sistemas	10/06/2017
RE002	Eliminar	Crear un protocolo de acceso al area	Area de sistemas	10/06/2017
RE003	Eliminar	Crear un protocolo de acceso	Area de sistemas	10/06/2017
RT004	Mitigar	Adquirir los equipos necesarios para el reslpado electrico	Area de sistemas	10/06/2017
RT005	Mitigar	Crear un proceso de adquisicion de tecnologias	Contabilidad	10/06/2017

Figura 4. Respuesta a los riesgos del proyecto

Fuente. Los Autores

4.2.2 Riesgos críticos evaluados por la auditoría. La auditoría centro la revisión en 5 riesgos que se consideraron críticos para el cumplimiento de los objetivos de la empresa TMSOFT S.A.S, los cuales son.

R01: Daños físicos en los equipos y perdida de información sustancial para la empresa debido a la falta de protocolos de respuesta en caso de incendio.

R02: Acceso no autorizado al cuarto de servidores por falta de políticas en el acceso del mismo.

R03: Acceso no autorizado a los equipos del personal debido a la falta de controles en el acceso a las instalaciones.

R04: Daños físicos y perdida de información sensible para la empresa por falta de mecanismos de contingencia en caso de cortes eléctricos.

R05: Afectación de la continuidad del negocio en caso de incidentes debido a la falta de planes de contingencia.

4.3. Planteamiento de la guía estratégica para el mejoramiento de seguridad física de la empresa Tmsoft S.A.S.

Para propender instalar una guía estratégica y mejorar la seguridad física de la empresa TMSOFT S.A.S, se dividió en tres faces su ejecución, para visualizar los avances y velar por el cumplimiento de los procesos que culminan con el cumplimiento del objetivo del trabajo de grado.

Introducción

En esta fase se hizo un trabajo de campo donde la prioridad fue tener todo el conocimiento de manera general acerca de la empresa y sus actividades, su recurso humano, sitio donde se ubica la empresa, estado de las instalaciones y equipos. Se captó información relevante como lo son los archivos permanentes y se realizó la reunión de apertura, con la cual, elaboramos

cuestionarios (Entrevista, check list), se programó y se ejecutó la entrevista al gerente del área de sistemas y se definió la metodología de la auditoria y la norma ISO/IEC 27001 en la cual, basamos el proyecto de grado.

Indagación y fundamentos de auditoria.

Al hablar de seguridad de la información, es proteger tanto la información como los sistemas de información, contra un gran número de amenazas como: acceso, uso, divulgación, interrupción o destrucción no autorizada, que atenta contra la continuidad de los servicios de toda organización. Para lograr mitigar los riesgos de seguridad, se establecen controles adecuados como políticas, procesos, procedimientos, estructuras organizativas y aplicaciones, entre otras, con el objeto de asegurar la continuidad del negocio, minimiza los riesgos y maximiza la utilidad y continuidad del negocio.

Para una adecuada gestión de la seguridad de la información, es necesario implantar un sistema que bordee esta tarea de forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización, éste tema es abordada por la Norma ISO/IEC 27000 que contiene un conjunto de estándares desarrollados por ISO (International organization for Standardization) e IEC (International Electrotechnical Commission) y proporcionan un marco de gestion de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La norma ISO/IEC 27001 un modelo para el establecimiento, implementación,

Operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización

están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

El enfoque presentado por esta norma, estimula a los usuarios en la importancia de:

a) comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información.

b) implementar y operar controles para manejar los riesgos de seguridad de la de información del negocio de una organización.

c) Seguimiento y revisión del desempeño y eficacia del SGSI.

d) Mejorar la continuidad basada en la medición de objetivos.

Esta norma adopta el modelo PVHA "Planificar-Hacer-Verificar-Actuar"

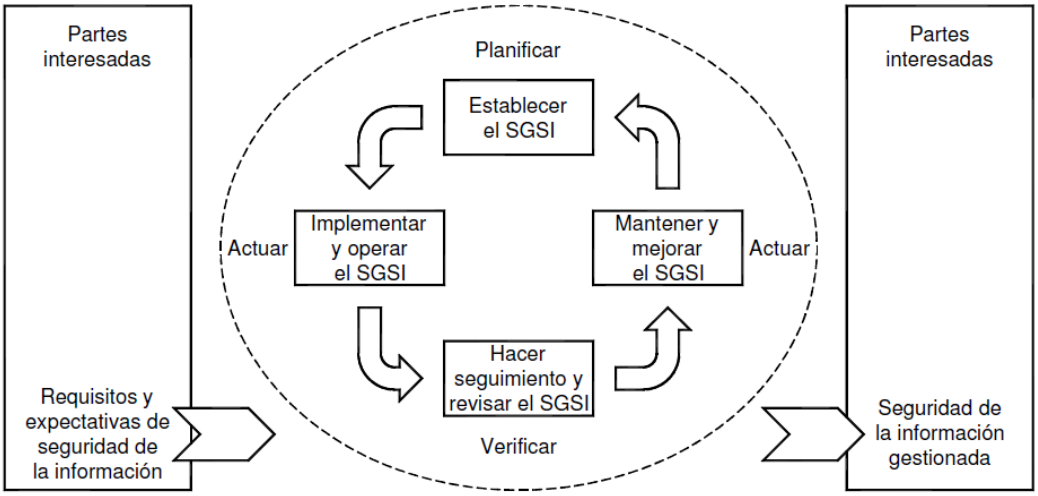

Figura 5. Ciclo PDCA

Fuente. http://www.pdcahome.com/5202/ciclo-pdca/

Tabla 3. Ciclo PDCA

CICLO	Descripción del Ciclo
Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente. http://www.pdcahome.com/5202/ciclo-pdca/

Nota: La siguiente tabla muestra ciclos de mejora continua que se basa en Planificar - Hacer – Verificar - Actuar.

Elaboración y socialización de la guía

En esta fase se trabajó en la elaboración de la guía con base en la experiencia y conocimientos que tenemos en el área de sistemas. Buscamos el material idóneo que proveerían a la empresa TMSOFT S.A.S de herramientas que garantizaran su seguridad física y ambiental y que le permitieran mantener continuidad y mitigar los riesgos que podría sufrir en el espacio y tiempo.

Elaborada la guía con todas las recomendaciones, se citó a una reunión al gerente de la empresa, el cual, desde el principio mostró su entusiasmo por ver los resultados del desarrollo de la auditoría y la posterior entrega de la guía. Con notorio entusiasmo recibió las instrucciones que como equipo mostramos y agradeció por escogerlos para desarrollar nuestro proyecto.

4.3.1 Guía para la seguridad física de la empresa TMSOFT S.A.S. Teniendo una base teórica para desarrollar la guía, se inicia su redacción.

Riesgos

Esta guía es una herramienta para identificar y gestionar los riesgos que corresponden a la seguridad física de la empresa TMSOFT S.A.S. la cual brinda un esquema que permite evaluar los riesgos y la seguridad de la información y los equipos tecnológicos que posee la organización.

Se toma como referencia es esquema de gestión de riesgos donde se evalúan los riesgos (Identifican, analizan y priorizan), al tiempo en que se controlan los riesgos (Reducir, planear solución, resolver)

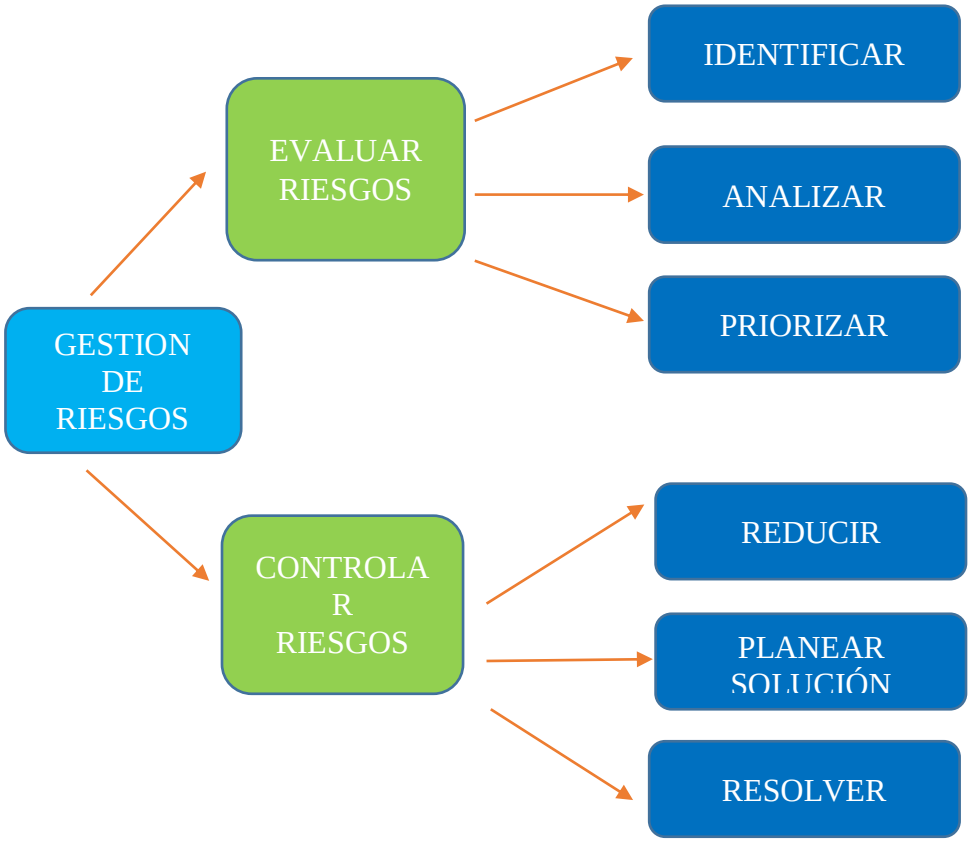

Figura 6. Gestión de riesgos

Fuente. Los Autores

Así también tomamos los tres principios de la seguridad de la información

Confidencialidad

Se conoce la confidencialidad como la forma de prevenir la divulgación de la información a personas o sistemas no autorizados.

Tomemos un ejemplo claro y conciso: Cuando hacemos una compra por internet con nuestra tarjeta de crédito, los datos de nuestra tarjeta (Número de identificación de la tarjeta y código de seguridad) viajan a través de la red por medio de un sistema cifrado el cual se comunica con el emisor de nuestra tarjeta y con el comerciante al cual le estamos haciendo la compra, si al hacer

este proceso una parte no autorizada obtiene estos datos de una forma fraudulenta, entonces allí se ha producido una divulgación de la información y se ha perdido la confidencialidad.

Pero no solo la perdida de la confidencialidad se da en los sistemas de información, el solo hecho de que una persona mire encima de su hombro para ver que hacemos en la pantalla de nuestro celular o netbook, cuando un equipo de cómputo es robado de una empresa, cuando información sensible es divulgada por cualquier medio sea digital o no.

Integridad

Hablar de integridad en Seguridad de la información, es hablar de cómo los datos se mantienen intactos libres de modificaciones o alteraciones por terceros (Personas no autorizadas), cuando una violación modifica datos en una base de datos de información, se sea por accidente o mala intención se pierde la integridad, y por ende falla el proceso.

Para esto debemos proteger la información de una manera que solo pueda ser modificada por la misma persona, o por personal autorizado, evitando así perder la integridad. Una forma de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña segura o la autenticación por medio de una huella digital, este último es de los medios más seguros que existen en la actualidad.

Disponibilidad

Es otro de los pilares fundamentales de la seguridad de la información, nada hacemos teniendo segura e integra nuestra información, si no va estar disponible cuando el usuario o un sistema necesite consultar la información.

Para cumplir esta última condición debemos tener muy claro que flujo de datos vamos a manejar, para saber dónde almacenar dicha información, que tipo de servicio debemos contratar, un servidor local, un servidor externo con varios clúster. Esto último depende de la cantidad de

información que manejemos, para esto se deben tener los conocimientos necesarios sobre base de datos y servidores, si no se tiene claro estos últimos conceptos lo mejor será buscar un experto.

4.3.2Análisis de los recursos

4.3.2.1 Inventario e infraestructura

Planos de la organización.

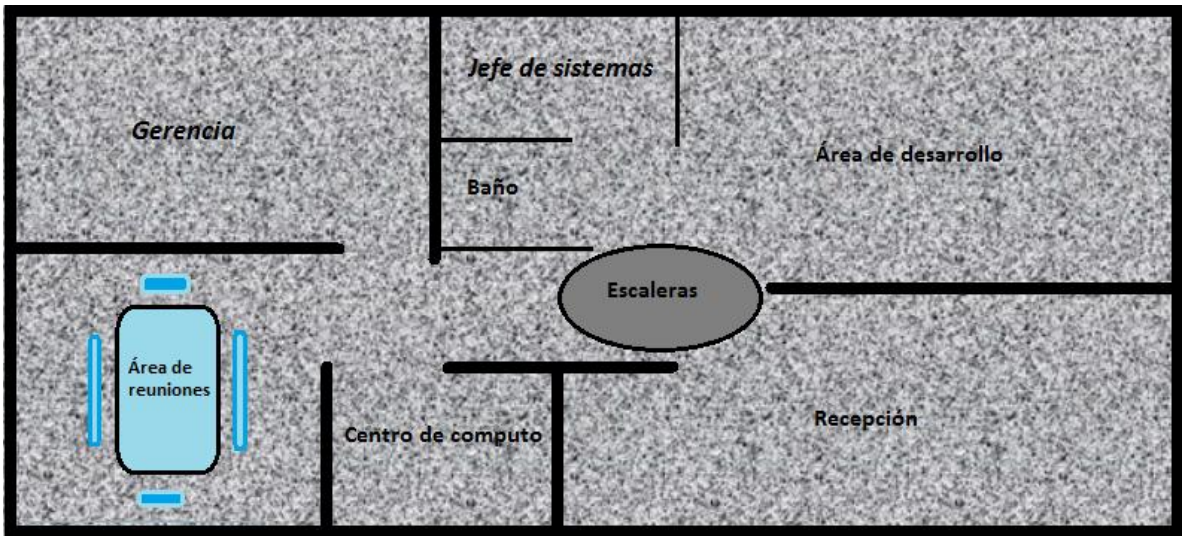

Figura 7. Plano de la Organización

Fuente. Los Autores

Inventario físico de la empresa

Se refleja el inventario del equipamiento físico de la empresa.

HARDWARE	
Cantidad	Especificaciones
3	Lenovo C440 ,CPU Intel® Pentium® G645 (doble núcleo / 2 threads, 2.90GHz, 3MB cache) Sistema operativo Windows 8 64-bit Intel HD Graphics
2	Servidor Hp ML210 Intel® Xeon® E3-1200v5 familia de productos Núcleo de procesador disponible 4, Caché de procesador L3 de 8 MB Velocidad del procesador 4,0 GHz, Formato (totalmente configurado) 4 U
1	Microserver Hp Familia del procesador Intel® Celeron®Caché de procesador 2 MB
	L3Velocidad del procesador 2,5 GHz
1	Router Monvistar
1	Router Directv
1	Switch Cisco
1	Microtik Router

Figura 8. Inventario físico de la empresa

Fuente. Los Autores

Propósito de la guía

RIESGOS	
Proyección de auditoria	Debido a la identificación de los riesgos existentes, se espera mejorar la seguridad física de la empresa TMSOFT S.A.S. para contar con los recursos necesarios para seguir siendo competitiva en el mercado del desarrollo
Fecha de inicio	21-ene-17
Fecha de finalización	21-abr-17
Propiedad	Grupo auditor: Jose Luis Quintero García-Jose Luis Martínez Mendoza

Figura 9. Riesgos

Fuente. Los Autores

ESTRATEGIA	
Proyección de auditoria	Terminada la auditoria y generada la guía, puesta en marcha de las estrategias formuladas para optimización de los procesos.
Fecha de inicio	21-ene-17
Fecha de finalización	21-abr-17
Propiedad	Grupo auditor: Jose Luis Quintero García-Jose Luis Martínez Mendoza
Colaboradores	Director Proyecto: Andrés Mauricio Puentes

Figura 10. Estrategia

Fuente. Los Autores

Guía de controles para mitigación de riesgos

CONTROLES SUGERIDOS			
CODIGO	ADMINISTRATIVO	OPERATIVO	DETALLE
CS-001	X		Reportes informativos sobre las políticas y normas dentro de la oficina.
CS-002		X	Poner en los vidrios de las ventanas, una película protectora contra rayos solares.
CS-003		X	Cambiar el sistema de la cerradura.
CS-004		X	Colocar video cámaras en la empresa.
CS-005	X		Colocar un sistema de alarma con un servidor de confianza.
CS-006		X	Dar una mejor ubicación al Data Center con un sistema de lector de huella para limitar el acceso.
CS-007		X	Dotar el área de sistemas con extintores adecuados para este tipo de área.
CS-008	X		Llevar registro de los cambios en privilegios para acceso de los usuarios.
CS-009	X		Llevar un inventario de los equipos.

Figura 11. Controles de la empresa

Fuente. Los Autores

4.3.3 Controles y sugerencias basados en la Norma ISO/IEC 27001

Tabla 4.

Políticas de seguridad de la información

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
A.5.1 GESTIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN			
A5.1.1	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	**CONTROL**	**RECOMENDACIONES**
	Políticas de la seguridad de la información	La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.	Crear un manual con todas las políticas de seguridad de la empresa. Socializar el manual de políticas de seguridad con el personal.
A5.1.2	Revisión de las políticas de seguridad de la información	Control Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.	Recomendaciones Socializar el manual en periodos de un año, preferiblemente, cuando el empleado cumpla el año de contrato.

Fuente. Los Autores

Nota: La siguiente tabla muestra los controles y recomendaciones realizadas a la empresa TMSOFT S.A.S, según la NORMA ISO/IEC 27001 para las Políticas de Seguridad de la Información.

Tabla 5. Seguridad física y de Medio Ambiente.

A.11 SEGURIDAD FÍSICA Y MEDIOAMBIENTAL			
A.11.1 ÁREAS SEGURAS **OBJETIVO: EVITAR ACCESOS FISICOS NO AUTORIZADOS, DAÑOS E INTERFERENCIAS CONTRA LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN Y LA INFORMACION DE LA ORGANIZACIÓN**			
A.11.1.1	**PERÍMETRO DE SEGURIDAD FÍSICA**	**CONTROL**	**RECOMENDACIONES**
		Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.	Estas áreas debes estas protegidas por Cámaras, alarmas y barreras físicas. Para exteriores: Cámara HD 1080P IR 40M DS-2CE16D5T-IT3 Hikvision y un DVR HIKVISION DS-7204 HQHI-F1 TURBO HD. Cambiar la puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero.
A11.1.2.	Controles físicos de los ingresos	Control Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.	Recomendaciones Para tener un control de acceso al área de sistemas se sugiere Usar una cerradura biométrica preferiblemente una cerradura L7000 Se recomienda una cámara HIKVISION DS-2CE56D8T-(A)ITZE para interiores Impedir el paso a personal no autorizado.

A11.1.3.	Seguridad de las oficinas, salas e instalaciones	Control Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	Recomendaciones Utilizar cámaras de seguridad para interiores preferiblemente HIKVISION DS-2CE56D8T-(A)ITZE. Para exteriores, Cámaras HD 1080P IR 40M DS-2CE16D5T-IT3 Hikvision y un DVR HIKVISION DS-7204 HQHI-F1 TURBO HD. Cambiar la puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero.
A11.1.4.	Protección contra las amenazas externas y medioambientales	Control Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.	Recomendaciones Se sugiere contar con extintores a la mano, limitados por una línea de fuego y formar al personal para su uso correcto. Teniendo en cuenta la fecha de caducidad de ellos. Contar con una alarma de fuego que se pueda manejar manualmente en caso de falsa alarma. Contar con una línea telefónica desde la que los empleados puedan llamar en caso de fuego. Prohibir el uso de cigarrillo. Mantener el área de sistemas limpia en la medida que sea posible. Limpiar periódicamente los filtros del aire de los ordenadores. Utilizar una aspiradora o un compresor periódicamente para retirar el polvo de los equipos de cómputo. Para casos de peligros ambientales Evitar colocar las máquinas en superficies muy altas, como por ejemplo, en lo alto de los gabinetes.

	No colocar objetos pesados en lugares que puedan caer sobre los equipos. No colocar los equipos junto a las ventanas. Considerar la posibilidad de sujetar los equipos físicamente a la superficie sobre la que reposan. Se sugiere que los backups estén almacenados en cajas de seguridad que soporten impactos. Para los se sugiere mantener una temperatura entre 15 y 25 º C (según recomendación del fabricante). Comprobar la documentación de los equipos para comprobar la temperatura a la que operan mejor. Instalar alarmas de temperatura en la sala de ordenadores, y programarlas para que se disparen cuando la temperatura esté entre 3 a 5 ºC del límite establecido. Algunos sensores pueden realizar acciones adicionales, como realizar llamadas de teléfono a la persona adecuada. Prestar atención a la forma en que los equipos expulsan el calor y el recorrido del aire caliente en la sala de ordenadores. Considerar la necesidad de instalar sistemas de enfriamiento adicional, e instalarlos correctamente. Ser cuidadoso colocando ordenadores cerca de las paredes, de forma que se dificulte la circulación del aire. La mayoría de fabricantes recomiendan como mínimo entre 15 y 30 cm. de espacio abierto por cada lado. Si no es posible respetar estas

	dimensiones, reducir el límite de temperatura superior en 5ºC o más. Si se está transportando un ordenador en un día muy frio o caluroso, permitir al mismo alcanzar la temperatura de la habitación antes de encenderlo.

Fuente. Los Autores

Nota: La siguiente tabla muestra los controles y recomendaciones realizadas a la empresa TMSOFT S.A.S, según la NORMA ISO/IEC 27001 para la Seguridad Física y de Medio Ambiente.

Tabla 6. Equipos

A.11.2 EQUIPOS			
OBJETIVO: EVITAR LA PÉRDIDA, DAÑO, ROBO O ACTOS EN LOS QUE SE COMPROMETAN ACTIVOS Y LA INTERRUPCIÓN DE LAS OPERACIONES DE LA ORGANIZACIÓN.			
A.11.2.1	**UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS**	**CONTROL**	**RECOMENDACIONES**
	L	Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.	Se sugiere verificar que los equipos de cómputo tengan buena ventilación, un sitio totalmente seco y no corra peligros por humedad. Para tener un control de acceso al área de sistemas se sugiere Usar una cerradura biométrica preferiblemente una cerradura L7000. Es necesario cambiar puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero. Se sugiere Vigilancia mediante personal y circuitos cerrados de televisión.
A.11.2.2	Servicios públicos de soporte	Control Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.	Recomendaciones Usar un buen sistema de protección eléctrica, preferible usa un buen UPS (Unit Power Supply = Sistema de Alimentación Ininterrumpida). De 3000 VA

			Toma corrientes con polo a tierra. Verificar que el voltaje que tenga el flujo eléctrico sea el requerido por los equipos(Generalmente 110 V)
	Seguridad en el cableado	Control Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.	Recomendaciones Usar un buen sistema de protección eléctrica, preferible usa un buen UPS (Unit Power Supply = Sistema de Alimentación Ininterrumpida). De 3000 VA. Los cables deben estar bien organizados y sin invadir el área de trabajo. Verificar que los tomas corrientes estén en buen estado.
A.11.2.4	Mantenimiento de los equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	Recomendaciones Mantenimiento preventivo a los equipos mínimo una vez al año. La persona o empresa que realice la labor de mantenimiento debe contar con certificación.
A.11.2.5	Retiro de los activos	Control El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización	Sugerencias Contar con vales de entrada y salida de equipos bajo revisión y firma del jefe del área.

Fuente. Los Autores

Nota: La siguiente tabla muestra los controles y recomendaciones realizadas a la empresa TMSOFT S.A.S, según la NORMA ISO/IEC 27001 para los Equipos.

A.5 Políticas de seguridad de la información			
A.5.1 Gestión de la Gerencia para la seguridad de la información			
A5.1.1	Políticas de la seguridad de la información	Control La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.	Recomendaciones Crear un manual con todas las políticas de seguridad de la empresa. Socializar el manual de políticas de seguridad con el personal.
A5.1.2	Revisión de las políticas de seguridad de la información	Control Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.	Recomendaciones Socializar el manual en periodos de un año, preferiblemente, cuando el empleado cumpla el año de contrato.

Figura 12. Políticas de seguridad de la información

Fuente. ISO 27001:2013

A.11 Seguridad física y medioambiental			
A.11.1 Áreas seguras			
Objetivo: evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización			
A.11.1.1	Perímetro de seguridad física	Control Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.	Recomendaciones Estas áreas debes estas protegidas por Cámaras, alarmas y barreras físicas. Para exteriores: Cámara HD 1080P IR 40M DS-2CE16D5T-IT3 Hikvision y un DVR HIKVISION DS-7204 HQHI-F1 TURBO HD. Cambiar la puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero.
A11.1.2.	Controles físicos de los ingresos	Control Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.	Recomendaciones Para tener un control de acceso al área de sistemas se sugiere Usar una cerradura biométrica preferiblemente una cerradura L7000 Se recomienda una cámara HIKVISION DS-2CE56D8T-(A)ITZE para interiores Impedir el paso a personal no autorizado.
A11.1.3.	Seguridad de las oficinas, salas e instalaciones	Control Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	Recomendaciones Utilizar cámaras de seguridad para interiores preferiblemente HIKVISION DS-2CE56D8T-(A)ITZE. Para exteriores, Cámaras HD 1080P IR 40M DS-2CE16D5T-IT3 Hikvision y un DVR HIKVISION DS-7204 HQHI-F1 TURBO HD. Cambiar la puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero.

A11.1.4.	Protección contra las amenazas externas y medioambientales	Control Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.	Recomendaciones Se sugiere contar con extintores a la mano, limitados por una línea de fuego y formar al personal para su uso correcto. Teniendo en cuenta la fecha de caducidad de ellos. Contar con una alarma de fuego que se pueda manejar manualmente en caso de falsa alarma. Contar con una línea telefónica desde la que los empleados puedan llamar en caso de fuego. Prohibir el uso de cigarrillo. Mantener el área de sistemas limpia en la medida que sea posible. Limpiar periódicamente los filtros del aire de los ordenadores. Utilizar una aspiradora o un compresor periódicamente para retirar el polvo de los equipos de cómputo. Para casos de peligros ambientales Evitar colocar las máquinas en superficies muy altas, como por ejemplo, en lo alto de los gabinetes. No colocar objetos pesados en lugares que puedan caer sobre los equipos. No colocar los equipos junto a las ventanas. Considerar la posibilidad de sujetar los equipos físicamente

Figura 13. Seguridad física y de Medio Ambiente

Fuente. ISO 27001:2013

A.11.2 Equipos			
Objetivo: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.			
A.11.2.1	Ubicación y protección de los equipos	Control Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.	Recomendaciones Se sugiere verificar que los equipos de cómputo tengan buena ventilación, un sitio totalmente seco y no corra peligros por humedad. Para tener un control de acceso al área de sistemas se sugiere Usar una cerradura biométrica preferiblemente una cerradura L7000. Es necesario cambiar puerta y cerradura de ingreso a la empresa. La puerta debe ser de acero forjado y una cerradura con sistema Medeco en acero. Se sugiere Vigilancia mediante personal y circuitos cerrados de televisión.
A.11.2.2	Servicios públicos de soporte	Control Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.	Recomendaciones Usar un buen sistema de protección eléctrica, preferible usa un buen UPS (Unit Power Supply = Sistema de Alimentación Ininterrumpida). De 3000 VA. Toma corrientes con polo a tierra. Verificar que el voltaje que tenga el flujo eléctrico sea el requerido por los equipos(Generalmente 110 V)
	Seguridad en el cableado	Control Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.	Recomendaciones Usar un buen sistema de protección eléctrica, preferible usa un buen UPS (Unit Power Supply = Sistema de Alimentación Ininterrumpida). De 3000 VA. Los cables deben estar bien organizados y sin invadir el área de trabajo. Verificar que los toma corriente estén en buen estado.
A.11.2.4	Mantenimiento de los equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	Recomendaciones Mantenimiento preventivo a los equipos mínimo una vez al año. La persona o empresa que realice la labor de mantenimiento debe contar con certificación.
A.11.2.5	Retiro de los activos	Control El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización	Recomendaciones Contar con vales de entrada y salida de equipos bajo revisión y firma del jefe del área.

Figura 14. Equipos

Fuente. ISO 27001:2013

Referencias

Academy 27001. (2013). Que es la norma ISO 27001 (2). Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/

Alegsa Leandro (26 de febrero del 2010). Seguridad Física. Recuperado de http://www.alegsa.com.ar/Dic/seguridad_fisica.php

Villegas Jaime (22 de febrero del 2009). Sistema de Control de Acceso. Recuperado de https://www.tecnoseguro.com/faqs/control-de-acceso/%C2%BF-que-es-un-control-de-acceso.html

Ortega Ruiz Luis Hernando. (22 de Octubre de 2014). Concepto sobre amenazas, vulnerabilidad, riesgos y desastres. Recuperado de https://prezi.com/jqaa12sg1dq-/conceptossobreamenazas-vulnerabilidad-riesgos-y-desastres/

Vera Cortes Jessica Paola (6 de febrero 2016). Que son riesgos Informáticos. Recuperado de https://prezi.com/pzwpnvitwsfr/que-son-riesgos-informaticos/

Fernandez Silvia. (29 de Noviembre de 2015). InformáticaEstudio, Servidores-Tipos de servidores. Recuperado de http://informaticaestudio.com.ar/2015/11/servidores-tipos-de-servidores/# more-972

Lerma Gonzales H. D. (2009). Metodología de la investigación: propuesta, anteproyecto y proyecto. Recuperado de https://books.google.com.co/books?id=COzDDQAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Hernández Sampieri, Fernández Collado, Baptista Lucio, (1997) Metodología de la investigación (1890) Recuperado http://www.dgsc.go.cr/dgsc/documentos/cecades/metodologia-de-lainvestigacion. pdf.

Socialización.

Para cumplir con los objetivos trazados, se citó nuevamente al gerente y al jefe de sistemas de la empresa TMSOFT S.A.S. para compartir todos los logros de auditoria y posterior elaboración de la guía que mitiga los riesgos a los que se expone la organización de no contar con ella.

Se hace entrega de un informe detallado del proyecto y la guía para el mejoramiento de la seguridad física de la empresa.

Conclusión

Durante el desarrollo de la auditoria se pudo constatar que la empresa carece de manera general de planes de contingencia en caso de emergencia, además de carecer de controles que permitan controlar el acceso a las áreas críticas de la empresa poniendo en riesgo tanto los activos físicos de la empresa como la fiabilidad e integridad de la información. Teniendo claro que la información y el personal son el activo más importante en toda organización no se puede escatimar en gastos ni esfuerzos para garantizar la seguridad de los mismos.

Recomendaciones

Se debe llevar acabo de manera periódica y programada procesos de auditoria que permitan continuar con el mejoramiento de la seguridad física y ambiental de la empresa logrando de esta forma un crecimiento estable y seguro de la misma.

La empresa debe hacer seguimiento a los riesgos y posibilidades de mejora encontrados en la auditoria con el fin de garantizar que sean mitigados en un lapso de tiempo prudente.

Los trabajadores deben ser constante mente capacitados en los planes de contingencia en caso de emergencia para garantizar que todos conozcan los protocolos a seguir en caso de una calamidad.

Apéndices

Apéndice A

Encuesta al personal del área de sistemas de la empresa TMSOFT S.A.S.

Objetivo:

Evaluar el conocimiento y los límites en seguridad que tiene la empresa TMSOFT S.A.S. basándonos en los requisitos para establecer un SGSI atreves de la norma NTC-ISO/IEC 27001.

1. ¿La empresa cuenta con un sistema de seguridad que proteja los equipos?

SI __ NO __

2. ¿Conoce o identifica usted ése sistema?

SI __ NO __

3. ¿Considera que el sistema de seguridad con que cuenta la empresa, garantiza la protección de los equipos?

SI __ No __

4. ¿existe una persona a cargo de la seguridad?

SI __ NO __

5. ¿La empresa ha sufrido de alguna intervención a la seguridad física o robo de sus equipos?

SI __ NO __

6. Si la respuesta a la anterior pregunta es si responda: ¿Se han adoptado medidas de seguridad que mitiguen los riesgos de una nueva intervención?

SI __ NO __

Apéndice B

Cuestionario para evaluar el nivel de la seguridad con que cuenta la empresa TMSOFT S.A.S.

Esta encuesta se realiza al jefe del área de sistemas.

1. ¿La cerradura para proteger la entrada en electrónica o mecánica?_____

_____

_____

2. ¿Posee algún sistema de seguridad o de alarma?

SI __ No __

3. ¿Cuentan con vigilancia las 24 horas?

SI __ NO __

4. ¿Qué medidas tiene para registrar el ingreso y salida del personal a la empresa?

-

_____

_____

_____

5. ¿El Data Center se encuentra bien ubicado?

SI __ NO __

6. ¿Posee cámaras de vigilancia dentro y fuera de la empresa?

SI __ NO __

7. ¿Cuenta con algún sistema de control para el ingreso al Data Center?

SI __ NO __

8. ¿ha establecido políticas de seguridad a sus empleados para un buen manejo de los equipos y la información de la empresa?

SI __ NO __

9. ¿Sus empleados tienen claras esas políticas?

SI __ NO __

10. ¿Cuenta con algún sistema de respaldo ante situaciones de riesgo?

SI __ NO __

Apéndice C

ENCUESTA **AC-4**	**EMPRESA: TMSOFT S.A.S.**
OBJETIVO: Establecer el conocimiento de las políticas y actividades que se realizan en el área de sistemas.	
FECHA DE ELABORACION: 19 de Diciembre de 2016	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
RESPONSABLE DEL AREA: Alexander Cruz Márquez	
CARGO: Jefe del área de sistemas	
AUDITORES: José Luis Quintero García (AA...1) **José Luis Martínez Mendoza (AA...2)**	
DIRIGIDO: Todo el personal que conforma el área de sistemas	
TIPO DE ENCUESTA: Preguntas cerradas	
PREGUNTA	**RESPUESTA** **SI/NO**
1. ¿Conoce los roles que se tienen definidos para el desarrollo de las funciones del área?	
2. ¿Conoce los mecanismos de control utilizados para verificar el cumplimiento de las actividades que realizan diariamente?	
3. ¿Existe un manual de funciones que documente las actividades que realizan diariamente en el desarrollo de sus funciones?	
4. ¿Sabe y conoce los métodos para la seguridad y protección de la información utilizados en la empresa?	
5. ¿Conoce las políticas de seguridad existentes para conservar la seguridad de la información?	
6. ¿Es capacitado constantemente de manera que este actualizado en el ejercicio de su labor?	

7. ¿Existe una persona responsable de la seguridad?	
8. ¿El centro de cómputo tiene salida al exterior?	
10. ¿Son controladas las visitas y demostraciones en el centro de Cómputo?	
11. ¿Se ha capacitado al personal en el manejo de los extintores?	
12. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	
13. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños a equipos?	
14. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?	
Elaborado	**José Luis Quintero García** **José Luis Martínez Mendoza**

Apéndice D

FORMATO DE OBSERVACION **AC-6**	**EMPRESA:** **TMSOFT S.A.S.**
FECHA DE ELABORACION: 19 de Diciembre de 2016	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
OBJETIVO: Revisar y Evaluar los controles, sistemas, procedimientos y funcionamiento del área de sistemas, para mitigar los riesgos que afecten de la seguridad física y ambiental de la información. **Objetivos específicos:**	

Conocer las actividades y el estado actual del área de sistemas. **Establecer los factores que ponen en riesgo la seguridad física y ambiental de la información.**
ALCANCE: Revisar todos los procedimientos establecidos en el área de sistemas verificando la existencia de controles y cumplimiento de las actividades estipuladas en cada una de las funciones del personal.
RESPONSABLE DELAREA: Alexander Cruz Márquez
CARGO: Jefe del área de sistemas
AUDITORES: José Luis Quintero García (AA...1) **José Luis Martínez Mendoza (AA...2)**
SITUACIONES OBSERVADAS EN EL DESARROLLO DE LA AUDITORIA:
FORTALEZA: Se evidencio en el trascurso de las visitas a la empresa, que el personal que labora en el área de sistemas tiene cada uno su puesto de trabajo en las condiciones adecuadas, así mismo que laboran mancomunadamente puesto que las actividades son de retroalimentación y una labor desarrollada, genera la consecución de otra actividad por parte de otro trabajador. **Así mismo se observa la disposición del jefe del área de sistemas y el gerente de la empresa.**

Apéndice E

RESUMEN DE DESVIASIONES DETECTADAS **AC-12**	**EMPRESA:** **TMSOFT S.A.S.**
FECHA DE ELABORACION: 19 de Diciembre de 2016	
AREA AUDITADA: Sistemas Desarrollo y Soporte	

Ref.	Situaciones	Causas	Solución
DDT.1	**Mecanismos que garanticen la seguridad física de los equipos.**	**Robo, fraude y mal uso de las instalaciones y medios.**	**Que se documenten y establezcan revisar los mecanismos por medio de los cuales el sitio genere las medidas necesarias para garantizar la seguridad de los equipos.**

DDT.2	**Condiciones no aceptables en las que se encuentren las servidores**	**Por falta de conocimiento y mantenimiento, generados por falta de revisión y cuidado del personal a cargo.**	**Implementación de estrategias que minimicen el impacto que se genera al no tener los servidores en condiciones adecuadas.**

ELABORÓ	
José Luis Quintero García **José Luis Martínez Mendoza**	

PROGRAMA DE AUDITORIA **AC-1**	**EMPRESA:** **TMSOFT S.A.S.**
FECHA DE ELABORACION: 4 de Enero de 2017	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
OBJETIVO: Revisar y Evaluar los controles, sistemas, procedimientos y funcionamiento del área de sistemas, para mitigar los riesgos que afecten la integridad de la seguridad de la información. **Objetivos específicos:** **Conocer las actividades y el estado actual del área de sistemas.** **Establecer los factores que ponen en riesgo la seguridad física y ambiental de la información.**	
ALCANCE: Revisar todos los procedimientos establecidos en el área de sistemas verificando la existencia de controles y cumplimiento de las actividades estipuladas en cada una de las funciones del personal.	
RESPONSABLE DELAREA: Alexander Cruz Márquez	
CARGO: Jefe del área de sistemas	
AUDITORES: José Luis Quintero García (AA...1)	

José Luis Martínez Mendoza (AA...2)					
FASE	**DESCRIPCION**	**ACTIVIDAD**	**FECHA INICIO**	**FIN**	**DIAS HABILES**
I	**FUNDAMENTOS DE AUDITORÍA** **Recolección de archivos permanentes** **Visita al área de sistemas** **Reunión de apertura** **Elaboración de cuestionarios(Entrevista, check list)** **Programación de la entrevista al gerente del área de sistemas**	**-Visita inicial**	**20/12/2016**	**24/12/2016**	**5 DIAS**
		-Presentación del equipo auditor.	**20/12/2016**	**24/12/2016**	
		-Solicitud de los documentos del área.	**20/12/2016**	**24/12/2016**	
		-Preparación de la lista de chequeo, entrevista al jefe del área y al jefe del área y encuesta y encuesta al personal de desarrollo y soporte	**20/0122016**	**24/12/2016**	
II	**DESARROLLO DE LA AUDITORÍA** **Desarrollar entrevista al jefe del del área de sistemas** **Realizar encuesta a empleados** **Realizar observación y check list.** **Analizar claves de acceso, control, seguridad, confiabilidad y copias de seguridad del área de sistemas**	**Realizar la entrevista al jefe del área de sistemas y encuesta a cada uno de los empleados que conforman el equipo de desarrollo y soporte. Así mismo mediante el método de observación establecer que controles y que actividades se realizan en dicho proceso, mediante el cumplimiento de la lista de chequeo.**	**09/01/2017** **09/01/2017**	**15/01/2017** **15/01/2017**	**7 DIAS**
		Revisión de los documentos del área, como manuales y procedimientos, revisión del cumplimiento de las etapas establecidas para sus actividades.	**09/01/2017**	**15/01//2017**	

	Evaluación física	**Revisión de los mecanismos de socialización al personal sobre los manuales y procedimientos establecidos**	**09/01/2017**	**15/01//2017**	
III	**EJECUCIÓN DE PRUEBAS Se realiza el resumen de desviaciones detectadas y situaciones encontradas así mismo se elaboran las pruebas**	**Análisis de los papeles de trabajo Revisiones de las situaciones encontradas y detectadas acuerdo con las evidencias y lo encontrado en el desarrollo de la auditoria.**	**23/012017**	**26/01/2017**	**4 DIAS**
IV	**INFORME Elaboración del informe final.**	**Elaboración del dictamen, de acuerdo a los hallazgos obtenidos en la revisión.**	**10/02/2017**	**13/02/2017**	**3 DIAS**
V	**SOCIALIZACION Presentación del informe final**	**Una vez realizado el dictamen de la auditoria, se socializa con el jefe del área y con el jefe de la empresa, para exponer los resultados de la auditoria**	**22/02/2016**	**22/02/2017**	**1 DIA**
Elaborado: José Luis Quintero García José Luis Martínez Mendoza					

Apéndice F

ENTREVISTA **AC-3**	**EMPRESA: TMSOFT S.A.S.**

FECHA DE ELABORACION: 11 de Mayo de 2016	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
RESPONSABLE DEL AREA: Alexander Cruz Márquez	
CARGO: Jefe del área de sistemas	
AUDITORES: José Luis Quintero García (AA...1) **José Luis Martínez Mendoza (AA...2)**	
REGISTRO	**OBSERVACIÓN**
1. ¿Cómo está distribuida el área de sistemas?	**El área de sistemas está divida o compuesta por un jefe de la división, cuenta con ingenieros para el área de desarrollo soporte e instalación (Ing. de campo)**
2. ¿Cuáles son los roles que se tienen definido para el desarrollo de funciones en el área de sistemas?	**Tienen un jefe que es el que da las directrices del trabajo, hay tres ingenieros (Ing. desarrollador, Ing. de soporte, Ing. de campo)que estos son los tres roles definidos dentro del área**
3. ¿Cuáles son las actividades que realiza el personal de sistemas?	**Ellos tiene unas actividades y labores definidas, pero que en estos momentos no se encuentran documentadas**
4. ¿Qué mecanismos de control son utilizados para verificar el cumplimiento de las actividades según el manual de funciones?	**En este momento solo está el control del jefe. Existe un software de control de proyectos pero no lo han documentado los responsables. El jefe hace la verificación de los procesos y existe una retroalimentación en las tareas, al final de la jornada el jefe realiza una verificación de lo hecho por sus empleados en servidores de respaldo.**

5. ¿Qué métodos existen para la seguridad y protección física y lógica de la información?	**Toda la información tiene encriptación en los servidores, la información sensible está protegida en los servidores por firewall y copias de seguridad. Toda la configuración está protegida en otro data center, ubicado en otro país y de igual forma el código fuente.** **Todo se encuentra en la nube, nada físico en la empresa, los servidores están en EE. UU. En un data center Tierr IV, de estos no existe aún uno en Colombia.** **Así mismo Google notifica accesos a las cuentas y envía un mensaje cuando se intenta acceder a algún perfil.** **Están operando en México Bogotá, en algunas partes de Colombia, Perú EE. UU. Es una compañía marca Colombia, certificados por el ministerio de las tics como embajadores tecnológicos. Se llaman a sí mismos una empresa de emprendimiento.**
6. ¿Qué políticas de seguridad existen para conservar la integridad de la información?	**Existen niveles jerárquicos para acceder a la información, usuarios y contraseñas, perfiles de acceso con privilegios y reportes de cada movimiento y acción informático en el sistema.**
7. ¿Cada cuánto se capacita al personal y como evidencian el cumplimiento de estas políticas?	**No hay capacitaciones formales como tal. Las capacitaciones son de manera constante porque aprenden cosas nuevas cada día, debido a que la investigación y avance de la tecnología, lleva a los mismos funcionarios a permanecer a la vanguardia de lo que esta era moderna ofrece y su cumplimiento es evidenciado con los resultados de los objetivos propuestos.**

Apéndice G

LISTA DE CHEQUEO **AC-5**	**EMPRESA: TMSOFT S.A.S** 

OBJETIVO: Establecer el conocimiento de las políticas y actividades que se realizan en el área de sistemas.
FECHA DE ELABORACION: 19 de Enero de 2017
AREA AUDITADA: Sistemas Desarrollo y Soporte
RESPONSABLE DEL AREA: Alexander Cruz Márquez
CARGO: Jefe del área de sistemas
AUDITORES: José Luis Quintero García (AA...1) **José Luis Martínez Mendoza (AA...2)**

VERIFICACION	**SE REALIZA VERIFICACION**
Las características físicas del área de sistemas son seguras	
Conexión de los equipos del área de sistemas	
Coordinación dentro del área sobre los lineamientos implementados para la seguridad de la información	
Implementación de manuales procedimentales	
Evaluación de la existencia y uso de normas, resolución de base legal para el diseño del área de sistema	
Conoce quién coordina dentro de proceso los lineamientos implementados para la seguridad de la información	
Requerimientos de seguridad del área de sistemas	

Funcionamiento de los equipos del área de sistemas	
Iluminación	

Seguridad de los equipos	
Estado del área de sistemas	
Entrada y salida al área física es	

Manual e instructivos para capacitación en el área de sistemas	
Planes en caso de contingencia	

Contraseñas de ingreso	
Bitácora de acceso al área de sistemas	
Monitoreo de accesos al sistema	
Niveles de acceso y seguridad en la red	
Aprovechamiento de los recursos de red	
Perfiles de seguridad adecuados para ingreso al sistema	
Evidencia investigativa por parte de los equipos de trabajo	
Evidencia de control diario por parte del jefe	
Pruebas de seguridad a la información	
Evidencia de la actividad informática del equipo del área de sistemas	
Monitoreo de ingreso al área de sistemas	
Cronograma de trabajo para el área operativa	
Respaldo de la Información sensible para la empresa	
Espacio físico para el equipo desarrollador	

Apéndice H

FORMATO DE PRUEBA **AC-7**	TMSOFT BrainPower **EMPRESA:** **TMSOFT S.A.S**
FECHA DE ELABORACION: 23 de Enero de 2017	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
RESPONSABLE DELAREA: Alexander Cruz Márquez	
CARGO: Jefe del área de sistemas	
AUDITORES: José Luis Quintero García (auditor 2)	

José Luis Martínez Mendoza (auditor 3)	
PRUEBA	**Verificación de mecanismos que garantizan la seguridad física y ambiental de los equipos.**
OBJETIVO DE LA PRUEBA	**Verificar los mecanismos implementados que protegen la integridad de los equipos.**
TECNICA A EMPLEAR	**Observación** **Indagación informal**
TIPO DE PRUEBA	**1.De cumplimientos ()** **2.Sustantiva ()** **3. De doble finalidad (x)**
PROCEDIMIENTO A IMPLEMENTAR	**Se revisaran los mecanismos por medio de los cuales se protegen física y administrativamente los equipos, de las adversidades ambientales y del comportamiento inapropiado del personal.**
RECURSOS	**Humanos y físicos.**
RESULTADOS DE LA PRUEBA	
HALLAZGOS	**-No se cuenta con unas políticas de seguridad para que los usuarios tengan mejor uso de los equipos.** **-No se encontró un mecanismo de respuesta automática que permita emitir una alerta de posible intrusión a la empresa.** **-El edificio no cuentan con protección por contraseña y validación de identidad que restrinja el acceso de personal a la empresa y se lleve una bitácora de su salida y entrada de la organización.** **-Los equipos del área de desarrollo no cuentan con un mecanismo que no permita su fácil y rápida extracción del edificio.**

CAUSAS	**La empresa se encuentra con un alto nivel de desprotección de sus equipos, lo que puede acarrear un fácil acceso a él y sustracción de manera fácil y rápida de sus equipos.**
SITUACION DE RIESGO QUE GENERA	**Vulnerabilidades en la integridad y disponibilidad de la información**
RECOMENDACIONES	**Se recomienda la implementación de las siguientes practicas:** **-Implementar un sistema de control que permita verificar si el usuario entra o sale del edificio.** **-Realizar la adquisición de elementos que garanticen la seguridad y protección de los equipos y sus instalaciones.**

Apéndice I

FORMATO DE PRUEBA **AC-8**	 **EMPRESA:** TMSOFT S.A.S.
FECHA DE ELABORACION: 23 de Enero de 2017	
AREA AUDITADA: Sistemas Desarrollo y Soporte	
RESPONSABLE DELAREA: Alexander Cruz Márquez	
CARGO: Jefe del área de sistemas	
AUDITORES: José Luis Quintero García (auditor 1) José Luis Martínez Mendoza (auditor 2)	
PRUEBA	Verificación del espacio físico del data center
OBJETIVO DE LA PRUEBA	Verificar que las condiciones en las que se encuentran los servidores sean las adecuadas
TECNICA A EMPLEAR	Observación Indagación informal
TIPO DE PRUEBA	1.De cumplimientos () 2.Sustantiva () 3. De doble finalidad (x)
PROCEDIMIENTO A IMPLEMENTAR	Se realizara un inspección al cuarto de equipos de la empresa para poder determinar si las condiciones en las que trabajan estos equipos son las optimas
RECURSOS	Humanos
RESULTADOS DE LA PRUEBA **HALLAZGOS**	-Se constató que la ubicación de los equipos no es la adecuada ya que no cuenta con un acceso controlado y registrado. -Se observó que los equipos no tiene un sistema de refrigeración o ventilación adecuado haciendo evidente las altas temperaturas en el área ya mencionada

	-No se encontraron extintores cerca de los equipos lo que implica unos riegos inminentes de perdida de información y equipos en caso de incendio. -Se constató que los equipos del data center cuentan con respaldo eléctrico adecuado
CAUSAS	El espacio en el cual se encuentran los servidores y otros equipos no es adecuada y no cumple con las condiciones mínimas para el correcto funcionamiento de los mismos
SITUACION DE RIESGO QUE GENERA	Riesgo de daños físicos en los equipos y perdida de información sensible para el funcionamiento de la empresa
RECOMENDACIONES	Se recomienda la implementación de las siguientes practicas -Instalar un sistema de aire acondicionado que permita mantener la refrigerado el cuarto -Instalar medidores de temperatura y humedad -Instalar una cerradura electrónica que permita llevar el registro de los empleados que acceden al cuarto de servidores -Implementar una alarma contra incendios complementado con extintores de tipo Novec 1230 o FM200 / FE-13