ANALISIS Y GESTION DE RIESGOS AL SISTEMA DE INFORMACION DE LA EMPRESA TEXTIL DISEÑOS Y DOTACIONES OSIRIS S.A.S APLICANDO METODOLOGIA MAGERIT

GIOVANNY ERNESTO JIMENEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS 'ECBTI'
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMÁTICA
2018

ANALISIS Y GESTION DE RIESGOS AL SISTEMA DE INFORMACION DE LA EMPRESA TEXTIL DISEÑOS Y DOTACIONES OSIRIS S.A.S APLICANDO METODOLOGIA MAGERIT

GIOVANNY ERNESTO JIMENEZ URBANO

Monografía para optar al título de
Especialista en Seguridad Informática

Director de proyecto
Ing. Iván Arturo López

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS 'ECBTI'
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMÁTICA
2018

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

Firma Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Ibagué, 01 de mayo de 2018

DEDICATORIA

El presente proyecto está dedicado a Dios por brindarme la sabiduría necesaria para lograr las metas propuestas, a mi abuela materna Lucrecia Barrero Q.E.P.D, por haberme enseñado e influenciado para ser una mejor persona cada dia y a mis padres quienes siempre me han apoyando en todas las metas propuestas.

Giovanny Ernesto

AGRADECIMIENTOS

Giovanny Ernesto expresa sus más sinceros agradecimientos a:

Ing. Iván Arturo López por su colaboración, dedicación y disponibilidad en el desarrollo de esta monografía, por sus sabios consejos y brindar sus conocimientos para enriquecer y fortalecer mi experiencia educativa.

A todos y cada uno de los colaboradores de la Empresa textil Diseños y Dotaciones Osiris s.a.s, por compartir sus actividades en cuanto al objeto productivo y social de la empresa, por brindar los espacios necesarios para recolectar la información que permitió un conocimiento más amplio de la organización.

CONTENIDO

Pag

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pag.

GLOSARIO

ACTIVO: es un sistema construido con bienes y servicios, con capacidades funcionales y operativas que se mantienen durante el desarrollo de cada actividad socio-económica específica.[1]

AMENAZAS: todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.[2]

SISTEMA INFORMATICO: sistema de información que basa la parte fundamental de su procesamiento, en el empleo de la computación, como cualquier sistema, es un conjunto de funciones interrelacionadas, hardware, software y de Recurso Humano.[3]

VULNERABILIDAD: es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.[4]

CONTROLES: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.[5]

BOTNETS: Botnet es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas.

---

1 Wikipedia. la enciclopedia libre. Activo (contabilidad), {En linea}. {01 de mayo de 2018}, disponible en: (https://es.wikipedia.org/wiki/Activo_(contabilidad)).

2 Departamento de seguridad informática. Amenazas a la Seguridad de la Información. Universidad Nacionalde Luján, Luján, Buenos Aires, Argentina. {En linea}. {01 de mayo de 2018} Disponible en: (http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12).

3 Ecured. Conocimiento con todos y para todos. Sistema Informatico. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.ecured.cu/Sistema_inform%C3%A1tico)

4 CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

5 Ronquillo, Sixto. Controles en la seguridad de la información. {En linea}. {01 de mayo de 2018}, disponible en : (https://prezi.com/gkwjvmaeivtc/controles-en-la-seguridad-de-la-informacion/)

Los ordenadores son parte del botnet, llamados “bots” o “zombies”. No existe un número mínimo de equipos para crear un botnet. Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos.[6]

CIBERESPACIO: Se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir. La información se puede intercambiar en tiempo real o en tiempo diferido, y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar.[7]

CIBERDEFENSA: Ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informaticos y teleinformaticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.[8]

MAGERIT: es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la nformación, enfocada a las Administraciones Públicas.[9]

DISPONIBILIDAD: Es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.[10]

CONFIDENCIALIDAD: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información.[11]

---

6 Fisher, Dennis. Kaspersky Lab Daily. ¿Qué es un botnet?. {En linea}. {01 de mayo de 2018} Disponible en : (https://www.kaspersky.es/blog/que-es-un-botnet/755/)

7 Ecured. Conocimiento con todos y para todos. Ciberespacio. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.ecured.cu/Ciberespacio)

8 Ciberdefensa-Ciberseguridad Riesgos y Amenazas, {En linea}. {01 de mayo de 2018} Disponible en : (http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf)

9 Wikipedia. la enciclopedia libre. Magerit (metodología). {En linea}. {01 de mayo de 2018} Disponible en : (https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa))

10 Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

11 Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

INTEGRIDAD: es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.[12]

POLITICAS DE SEGURIDAD: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad. Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.[13]

INGENIERIA SOCIAL: es una técnica de hackeo utilizada para sustraer información a otras personas teniendo como base la interacción social, de tal manera que la persona vulnerada no se dé cuenta cómo u cuándo dio todos los datos necesarios para terminar siendo la víctima de un ataque informático. En esta práctica se recurre, principalmente, a la manipulación de la psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que, en la cadena de seguridad de la información, el ser humano es el eslabón más débil.[14]

SGSI: Se define como sistema general de la seguridad de la información,es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.[15]

RIESGO: es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.[16]

---

12 Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

13 Wikipedia. la enciclopedia libre. Politica de seguridad. {En linea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad)

14 Arbelaez, Ana. Ingenieria social: El hackeo silencioso. {En linea}. {02 de mayo de 2018} Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

15 Wikipedia. la enciclopedia libre. Sistema de gestión de la seguridad de la información. {En linea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n)

16 CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

RESUMEN

El presente documento tiene como propósito aplicar la metodología MAGERIT a la Empresa textil Diseños y Dotaciones Osiris s.a.s, con el fin de analizar las distintas amenazas y vulnerabilidades a la que se encuentra expuesta.

Como principio la información de la empresa es sin duda uno de sus mayores activos, la cual debe ser preservada no solo por sus características sino por el grado de importancia que representa para la misma, ya que de ella dependerán decisiones de gran importancia que pueden afectar de una manera sustancial las líneas de negocio. Se parte del hecho de realizar un reconocimiento general de la empresa historia, esquema organizacional e identificación de los activos informáticos, de esta manera poder realizar una identificación de las posibles amenazas.

Dado lo anterior se realizara un análisis de riesgos con los hallazgos encontrados para poder emitir sugerencias en cuanto a las amenazas detectadas y de esta manera sugerir distintos controles que actúen de manera eficaz ante un ataque al sistema informático de la empresa.

Palabras Clave: amenazas, sistema informático, vulnerabilidades, activos informáticos, controles.

ABSTRACT

The purpose of this document is to apply the MAGERIT methodology to the Osiris s.a.s textile design and equipment company, in order to analyze the different threats and vulnerabilities to which it is exposed.

As a principle, the information of the company is undoubtedly one of its greatest assets, which must be preserved not only for its characteristics but also for the degree of importance it represents for it, since decisions of great importance that may affect it will depend on it. in a substantial way the business lines. It starts from the fact of making a general recognition of the company's history, organizational scheme and identification of computer assets, in this way to be able to identify possible threats.

Given the above, a risk analysis will be performed with the findings found to be able to issue suggestions regarding the detected threats and in this way suggest different controls that act effectively in the event of an attack on the company's computer system.

Keywords: threats, computer system, vulnerabilities, computer assets, controls.

TITULO

ANALISIS Y GESTION DE RIESGOS AL SISTEMA DE INFORMACION DE LA EMPRESA TEXTIL DISEÑOS Y DOTACIONES OSIRIS S.A.S APLICANDO METODOLOGIA MAGERIT

INTRODUCCION

Las tecnologías de la información han transformado la manera de pensar y actuar en toda sociedad, introduciendo cambios estructurales permitiendo modelar cualquier tipo de objeto en forma de información, facultando de esta manera la manipulación por medios electrónicos, es por esta circunstancia que cada vez más las personas y entidades tanto privadas como gubernamentales se han hecho dependientes de la tecnología, mas puntualmente de la internet, lo cual hace que cualquier red sea vulnerable a un ciberataque que puede poner en riesgo la seguridad de cualquier organización.

Este trabajo se enfoca en el análisis y probabilidades de riesgos de la empresa textil Diseños y dotaciones Osiris S.A.S, de la misma manera resaltar los beneficios que traería la implementación de un método de detención de ataques, el cual permita evidenciar como en el ciberespacio existen amenazas latentes a la seguridad de la información de la organización, de esta manera analizar las deficiencias en cuanto a actividades y procedimientos dirigidos a la preservación de la seguridad de los sistemas de información.

1. DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Con la masificación de la internet en todo el mundo la dependencia de las personas y las instituciones cada vez se ha hecho más grande para poder desarrollar cualquier actividad, pero de tal manera han ido apareciendo distintas amenazas para vulnerar la seguridad de cualquier red corporativa a través de distintos métodos como los botnets, ataques DDOS, entre otros.

Diseños y dotaciones Osiris S.A.S al no contar con un análisis de riesgos y unos controles de seguridad establecidos se encuentra expuesto a diferentes vulnerabilidades como el espionaje corporativo, sabotaje, suplantación de identidad, robos a cuentas bancarias, denegación de servicios por parte de los servidores, puntos altamente vulnerables que hacen que la red corporativa quede a merced de la delincuencia electrónica.

Se maneja información correspondiente a pedidos de distintos clientes, diseños y logotipos, información financiera, contable y administrativa, en cuanto a las buenas prácticas en seguridad informática se logra evidenciar que no existe conocimiento previo y una cultura corporativa que permita asegurar de manera adecuada la integridad, disponibilidad y confidencialidad de la información.

1.2 FORMULACION DEL PROBLEMA

¿Cómo diseñar un sistema de seguridad con sus respectivos controles, con el fin de prevenir y minimizar las amenazas, vulnerabilidades y riesgos a la seguridad de la información de la empresa textil Diseños y Dotaciones Osiris s.a.s? .

2. JUSTIFICACION

La importancia de proteger la información de las organizaciones y personas que hacen uso de las herramientas tecnológicas y del ciberespacio, se han convertido en una de las prioridades de nuestra actualidad, la medidas que se deben tomar en cuanto a ciberdefensa son diversas, por tal motivo es importante desarrollar este proyecto con el propósito de prevenir y detener cualquier ataque informático a la red de datos y a la información de la empresa textil diseños y dotaciones Osiris S.A.S, identificando de manera eficiente al atacante y de esta manera evitar de una manera controlada la sustracción de información sensible de los equipos de cómputo que se encuentran en la organización.

La prevención de cualquier tipo de ataque informático en la organización se verá recompensada en la relación costos beneficios, un ataque informático previamente planeado y ejecutado con precisión se verá reflejado en un costo económico para la organización, la complejidad de recuperar la información implica un costo económico que la organización debe asumir para continuar con sus labores de manera cotidiana

Diseños y dotaciones Osiris S.AS. se verá beneficiada con este proyecto minimizando los riesgos y las diferentes amenazas, a la seguridad de la información, evitando convertirse en un blanco potencial para la sustracción de información sensible de cualquier índole.

La organización se beneficiara de manera positiva con el desarrollo de este proyecto ya que tendrán a su disposición controles y políticas de seguridad como línea de defensa ante ataques múltiples por parte de ciberdelincuentes o personas con altos conocimientos informáticos que buscan vulnerar de cualquier manera la red y sus sistemas de información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Minimizar el impacto de las intrusiones y ataques sobre la red corporativa de diseños y dotaciones Osiris S.A.S con el fin de prevenir la sustracción de información sensible del servidor principal y equipos de computo, por medio del análisis de riesgos, recomendaciones de seguridad y el establecimiento de controles de seguridad.

3.2 OBJETIVOS ESPECIFICOS

- Identificar el grado de vulnerabilidad de la red de datos frente a ciberataques, mediante revisión del estado actual de su sistema de información.

- Identificar los activos de información que son propiedad de diseños y dotaciones Osiris S.A.S.

- Determinar los riesgos y amenazas de los activos de información que son propiedad de diseños y dotaciones Osiris S.A.S.

- Plantear controles basados en la norma ISO27000:2013 a los riesgos identificados en diseños y dotaciones Osiris S.A.S

- Elaborar el informe gerencial con los resultados obtenidos durante el análisis de riesgos y divulgación de las recomendaciones de seguridad sugeridas para la organización diseños y dotaciones Osiris S.A.S.

- Proyectar políticas de seguridad, con base a los distintos controles sugeridos.

4. ALCANCES Y LIMITACIONES

4.1 ALCANCES

La presente monografía es un proyecto destinado a realizar un análisis de riesgos y su propósito es proponer un conjunto de políticas de seguridad haciendo uso de la metodología MAGERIT, con el fin de diseñar una propuesta, la cual queda a disposición de la empresa, pero es responsabilidad de la misma la respectiva implementación.

4.2 LIMITACIONES

Es apropiado dar a conocer que el desarrollo de la presente monografía no incluirá los temas descritos a continuación:

- No se realizara análisis a ningún tipo de algoritmo.
- No se realizaran valoración al código fuente del software utilizado por la empresa.
- No se dará evidencia de los resultados encontrados posterior a la posible implementación.
- Se propondrán un conjunto de políticas para ser entregadas a la gerencia de la empresa.
- No se realizara implementación, solo definirán las políticas y controles de seguridad, la implementación es decisión de la gerencia de la empresa.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

El siguiente proyecto tendrá como referencia los siguientes temas:

La identificación de las vulnerabilidades y amenazas sobre las redes de datos, son las principales variables que se identifican para realizar un diseño adecuado y optimo, se realiza una actividad exploratoria para conocer los distintos ataques que se presentan, clasificarlos y calcular una posible cantidad de amenazas latentes o incursiones presentadas durante un lapso de tiempo determinado y su modus operandi, el propósito es verificar e identificar estas amenazas que se encuentran actualmente en el ciberespacio, lograr la identificación de factores comunes que permitan evaluar y ejecutar medidas de control y prevención.

De acuerdo a la sección de noticias del sitio oficial www.pandasecurity.com durante el primer semestre del año 2017 se registro un incremento sorprendente en la cantidad de ciberataques a gran escala y amenazas contra la seguridad informática global, en ciberdefensa debemos plantear las distintas acciones de defensa que se caracterizan por ser de tipo activas pasivas, proactivas, preventivas y reactivas para asegurar el buen uso y negar los servicios y datos a personas u organizaciones no autorizadas, por esta razón se debe realizar identificación de las amenazas de acuerdo a su caracterización, se clasificaran en internas y externas, al ser de carácter interno implica un riesgo mucho mayor ya que sistemas de seguridad como los firewall serian poco efectivos ya que estas intrusiones se dan por algún usuario que tiene al menos un acceso mínimo a los datos o servicios, al ser externos implica que estos proviene fuera de la red local, muchos de estos se dan por falta de protección en equipos y equipos de red vulnerables.

Igualmente se puede clasificar los distintos ataques en amenazas por el efecto y por el medio utilizado, cuando se refiere a las amenazas por el efecto se debe clasificar de acuerdo a las siguientes variables (robo de información, destrucción de información, anulación del funcionamiento de los sistemas o efectos que tiendan a ello, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, robo de dinero, estafas, etc), cuando definimos que el ataque es por el medio utilizado se refiere al objeto usado para términos más prácticos serian virus o malware entre otros tales

como (worms, bots, adware, cookies, phishing, ingeniería social, denegación de servicio, spoofing de DNS, de IP, de DHCP, etc.)

En la temática de ciberseguridad se establecen las variables y acciones de carácter preventivo que tengan por objeto asegurar el uso de las redes propias y a su vez negarlo a terceros, creando políticas que permitan de la misma manera proteger los activos de una organización y a la comunidad en general.

El modelo nacional de riesgos del ministerio de las tecnologías de información y comunicación[17], bajo este instrumento se puede realizar un análisis sobre las diferentes variables y hallazgos encontrados que puedan ser cuantificables, de esta manera determinar el impacto y la vulnerabilidad en las áreas más críticas, su impacto sobre la confidencialidad de la información y la clasificación de los riesgos de acuerdo a como se vayan presentando e identificando, con el fin de analizar los patrones de ataque y la intensidad de los mismos.

Lo anteriormente expuesto con el fin de llegar hacer una revisión de la red local y su estructura, pruebas de seguridad para poder implementar los respectivos controles y definir las políticas de seguridad.

5.2 MARCO CONCEPTUAL

5.2.1 Disponibilidad de servicios: su finalidad es poder analizar, definir, planificar con el fin de mejorar todos los aspectos relacionados en cuanto a los servicios de tecnología informática, con la finalidad de garantizar infraestructura, procesos y herramientas adecuadas para cumplir las metas y objetivos propuestos.

5.2.2 Impacto: De qué manera los ataques generados hacia la infraestructura de red, servidores e información crítica, afectan de manera directa e indirecta las líneas de negocio de las instituciones.

5.2.3 Probabilidad de ataques: se puede catalogar como una posibilidad que un ataque llegue a presentarse, no se pretende afirmar que sucederá , pero existen un riesgo inminente si presentamos fallas de seguridad dentro de nuestro sistema informático, su finalidad es determinar el tipo de riesgo al que estamos expuestos y su grado de complejidad.

---

17 Gobierno Digital. Enterate. MinTIC desarrolla el Modelo Nacional de Riesgos y genera capacidades humanas en Seguridad Digital, {En linea}. {03 de mayo de 2018} Disponible en: (http://estrategia.gobiernoenlinea.gov.co/623/w3-article-61852.html)

5.3 ESTADO ACTUAL DE LA EMPRESA TEXTIL DISEÑOS Y DOTACIONES OSIRIS S.A.S

Para conocer el estado actual de la empresa se realiza una revisión de la documentación desde el momento de su constitución como sociedad y los servicios que presta a sus diferentes clientes, con el propósito de analizar la información y generar estrategias que permitan fortalecer la confidencialidad, fiabilidad e integridad de la información.

5.3.1 DESCRIPCION DE LA EMPRESA

5.3.1.1 Historia

DISEÑOS Y DOTACIONES OSIRIS S.A.S es una empresa netamente tolimense, fundada en la ciudad de Ibagué en el año 2012, iniciando como un pequeño taller textil, el cual desde su inicio se trazó como objetivo principal la elaboración y comercialización de prendas de uso hospitalario al igual a todo lo referente en moda casual y actual, la empresa cuenta con un equipo de personas entre las que se encuentran madres cabezas de familia, las cuales se encargan de aportar su experiencia y habilidades en el desarrollo de costuras y prendas de alta calidad.

Actualmente DISEÑOS Y DOTACIONES OSIRIS S.A.S es una empresa en proceso de desarrollo que se caracteriza por la calidad de sus productos y servicios, utilizando la mejor materia prima, recursos humano de gran experiencia y brindando soluciones efectivas y adaptables a cualquier necesidad.

5.3.1.2 Misión

Somos una organización dedicada a la elaboración y comercialización de prendas de uso hospitalario y empresarial al igual a todo lo referente en moda casual y actual; dirigida a grandes, mediana y pequeñas empresas a nivel nacional.

Contamos con un talento humano conformado por personas idóneas, integras y comprometidas con su trabajo, que apoyándose en su experiencia, logran satisfacer de manera óptima las necesidades de nuestros clientes, trabajando siempre con honestidad, responsabilidad y cumplimiento.

5.3.1.3 Visión

En el año 2020 seremos reconocidos a nivel nacional como una de las empresas más grandes e importantes en elaboración y comercialización de prendas de uso hospitalario y empresarial al igual en todo lo referente en moda casual y actual, distinguiéndonos por la variedad y calidad de nuestros productos.

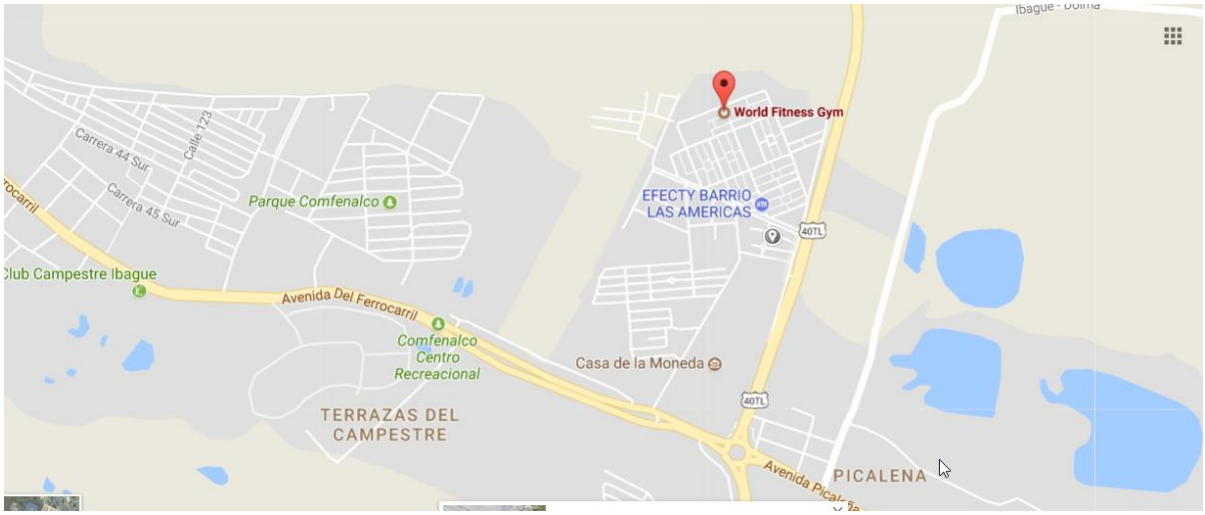
Implementaremos un portal en internet, con el fin de prestar un servicio de mayor cobertura, agilidad y de fácil acceso para nuestros clientes, contando con un talento humano caracterizado por su liderazgo, experiencia y compromiso con su deber.

5.3.1.4 Ubicación Geográfica

Diseños y dotaciones Osiris s.a.s tiene como domicilio principal la ciudad de Ibagué, al ser una empresa en crecimiento se proyecta cubrimiento a nivel nacional.

Dirección: supermanzana 10 manzana 19 casa 29, en el Barrio las américas

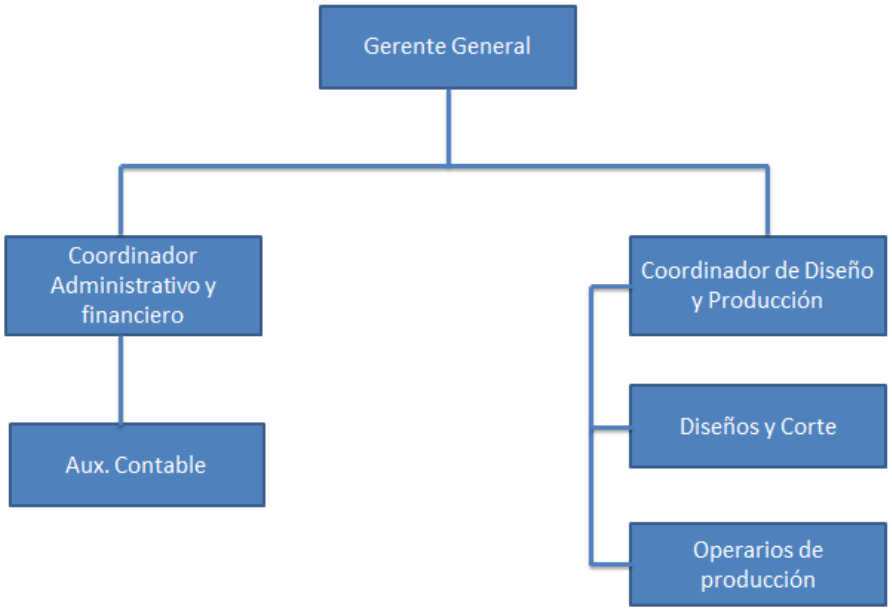
Figura 1. Ubicación geográfica de Diseños y dotaciones Osiris S.A.S



Fuente: Google Maps

5.3.2 ESTRUCTURA ORGANIZACIONAL

Figura 2. Organigrama



Fuente: El autor

5.3.3 FUNCIONES

GERENTE GENERAL

1) Representar a la sociedad ante terceros y ante las distintas autoridades de orden administrativo y judicial.
2) Ejecutar todos los actos administrativos que correspondan al objeto social, conforme a la legislación vigente.
3) Autorizar todos aquellos documentos que se generan para el desarrollo de las actividades de la organización.
4) Nombrar y remover empleados de la organización de acuerdo a las políticas de la organización.
5) Impartir ordenes e instrucciones a coordinadores y empleados para llegar al buen desarrollo de las actividades en pro de la organización
6) Cumplir y hacer cumplir todos los requisitos y exigencias legales que se relacionen con las actividades y funcionamiento de la organización.
7) Hacer cumplir el reglamento interno de trabajo.

COORDINADOR ADMINISTRATIVO Y FINANCIERO

1) El ultimo día de cada mes se realizara cierre contable y se generara un balance de prueba pormenorizado de las cuentas de la organización el cual se presentara al gerente general
2) Es la persona directamente responsable de la caja menor y de dar trámite del reembolso de la misma.
3) Revisar y verificar toda documentación de origen contable antes de ser avalada por el gerente general.
4) Verificar el todo el proceso contable generado por la organización.

COORDINADOR DE DISEÑO Y PRODUCCION

1) Verificar los diseños y muestras de cada uno de los productos solicitados por los clientes o que por incentivo propio genere la organización.
2) Establecer los patrones de diseño que debe usar el área de diseño y corte.
3) Verificar, parametrizar e instar a los operarios de producción para que cumplan las metas establecidas por la gerencia general.
4) Verificar el inventario de prendas listas para ser entregadas, así como el inventario de prendas con defectos de producción.

5.3.4 SISTEMAS DE INFORMACIÓN

La organización genera información contable la cual se ingresa a través de un sistema contable llamado ContaPyme[18], a través de este sistema se genera toda la facturación correspondiente a cada uno de los clientes, así como los diferentes activos, pasivos, gastos e ingresos provenientes del objeto social, de acuerdo a las normas internacionales de información financiera NIIF[19].

Ademas se cuenta con el software optitex[20], un software de diseño utilizado por diseñadores y empresas dedicadas a la elaboración de prendas, Permite ver sus diseños en pantalla mientras los está digitalizando. Puede agregar o quitar piezas. Trazo de curvas perfectas. El patrón que trabaja lo puede ver en el maniquí.

---

18 Contapyme NIIF. ContaPyme® Software administrativo y contable para pymes. Que es contapyme? {En linea}. {03 de mayo de 2018} Disponible en: (https://www.contapyme.com/software-contable/)
19 Gestion. Las Normas Internacionales de Información Financiera (NIIF). {En linea}. {03 de mayo de 2018} Disponible en : (https://gestion.pe/tendencias/normas-internacionales-informacion-financiera-niif-51948)
20 El costurero de stella. Que es optitex?. {En linea}. {03 de mayo de 2018} Disponible en: (https://www.elcosturerodestellablog.com/2009/03/que-es-optitex.html)

5.3.5 SERVICIOS QUE PRESTAN

Diseños y dotaciones Osiris s.a.s, presta servicios de elaboración y comercialización de dotaciones completas que incluyen prendas de uso hospitalario y empresarial al igual a todo lo referente en moda casual y actual, utilizando los mejores insumos para una optima producción y entrega a satisfacción del cliente.

5.3.6 PROCEDIMIENTOS ACTUALES

Actualmente la empresa Diseños y dotaciones Osiris s.a.s, solo cuenta con un único procedimiento de seguridad el cual consiste en realizar escaneo a memorias USB y realizar copias de seguridad a los archivos mas prioritarios, el software contable es el único que cuenta con un mecanismo de autenticación propio.

5.4 REFERENTES HISTORICOS

En el año 2012 se realizó análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de Pereira s.a e.s.p, basados en la norma iso 27005, en el cual se logra identificar, el riesgo existente en cuanto a seguridad de la información ya que no se cuenta con las medidas de seguridad apropiadas para resguardar y respaldar la información existente, la criticidad de los activos de información involucrados, así como la planificación de los procesos e identificación del valor estratégico del proceso de información del negocio.[21]

En el año 2017 se realizo análisis y gestión de riesgos en el marco del sgsi, basado en la metodologia magerit y apoyado en un api web para su ejecución en la PYME TrackSpia S.A.S, empresa que se dedica al mercado del rastreo satelital, durante este análisis utilizando la metodología magerit se lograra evidenciar las diferentes estrategias y políticas de la organización en cuanto a seguridad de la información y gestión del riesgo informático tales como lo son dominios, identificación de activos, valoración de activos, amenazas, valoración de amenazas, riesgo e impacto, y las salvaguardas.[22]

---

21 ANGARITA VIVAS, Alexis Armando. TABARES ISAZA, Cesar Augusto. Análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de pereira s.a e.s.p, basados en la norma iso 27005. Pereira, 2012, 104p. Proyecto de Grado para optar por el título de Especialista en Redes de Datos. Universidad tecnológica de Pereira. facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación

22 GARCIA HERNANDEZ, David Alejandro. RUIZ MURILLO, Jeisson Herley, analisis y gestion de riesgos en el marco del sgsi, basado enla metodologia magerit y apoyado en un api web para su ejecucion. Bogota, 2017, 225p. Monografía de grado para ingeniería telemática. Universidad distrital francisco josé de caldas. Facultad tecnológica ingenieria en telematica

6. DISEÑO METODOLOGICO

6.1 UNIDAD DE ANALISIS: DISEÑOS Y DOTACIONES OSIRIS S.A.S.

6.1.1 Población y muestra.

6.1.1.1 Población: 8 Empleados que hacen parte de la empresa Diseños y dotaciones Osiris s.a.s.

6.1.1.2 Muestra: 100% de la población ya que representa la totalidad de los empleados con los que cuenta actualmente la organización.

6.1.2 Estudio Metodológico. Investigación proyectiva., Este tipo de investigación, consiste en la elaboración de una propuesta, un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo.[23]

6.1.3 Marco Legal

6.1.3.1 Ley 1273 de 2009

Por medio de la cual se modifica el código penal creando un nuevo bien jurídico 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”.[24]

CAPÍTULO II

•Hurto por medios informáticos y semejantes
•Transferencia no consentida de activos

---

23 Investigación Holistica. La investigación proyectiva. {En linea}. {03 de mayo de 2018} Disponible en: (http://investigacionholistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html)
24 Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009. {En linea}. {03 de mayo de 2018} Disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

6.1.3.2 ISO 27000

En Colombia, las normas internacionales en seguridad de la información, han sido adoptadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC y el Gobierno Colombiano ha generado normativas de control interno como el MECI1000 y de calidad como la NTCGP1000 apoyado por estándares internacionales (COSO, ISO9001 respectivamente).
Las normas NTC ISO/IEC 27001 y NTC ISO/IEC 27005 fueron liberadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC en el año 2006 y 2008 respectivamente y son una copia idéntica por traducción de las normas ISO/IEC 27001 e ISO/IEC 27005. Estas normas permiten diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos. La norma NTC ISO/IEC 27001 adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, SGSI.
COSO, un marco de referencia para el control interno, es la base del modelo de control interno MECI1000, adoptado mediante el Decreto 1599 de 2005. Y COBIT, un marco de referencia para el Gobierno y control de TI basado en un modelo de procesos de TI alineado con COSO mediante la ISO9000 y la ISO27002. La ISO 9000 es el estándar para gestión de calidad en las organizaciones que fue trasladado a las entidades del Estado en la NTCGP 1000, adoptada mediante el Decreto 4140 de 2004 y actualizada mediante el Decreto 4485 de 2009.[25]

6.1.3.3 LEY 1266 DE 2008

Dicta disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.[26]

25 Ministerio de Tecnologías de la Información y las Comunicaciones. normativa del gobierno electrónico en Colombia. {En linea}. {03 de mayo de 2018} Disponible en: (http://viejoprograma.gobiernoenlinea.gov.co/apc-aa-files/5686d2a87532a21a70ead773ed71353b/NormativaGEL.pdf)
26 Alcaldia Mayor de Bogota. Regimen Legal de Bogota D.C. Ley 1266 de 2008 Nivel Nacional. {En linea}. {03 de mayo de 2018} Disponible en : (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488)

7. IDENTIFICACION DE ACTIVOS TECNOLOGICOS

Durante el proceso de identificación de los activos se puede obtener un criterio más sólido para lograr identificar las amenazas potenciales y de esta manera poder brindar la debida protección de los activos con los que cuenta la organización

7.1 CLASIFICACION DE LA INFORMACIÓN

La siguiente clasificación es determinada de acuerdo a la metodología MAGERIT en el libro II – Catalogo de elementos de la página 8 a 13.

7.1.1 [D] Datos / Información, La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. [27]

7.1.2 [K] Claves criptográficas, La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.[28]

7.1.3 [S] Servicios, Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.[29]

7.1.4 [SW] Software - Aplicaciones Informáticas, Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.[30]

---

27 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
28 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
29 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
30 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

7.1.5 [HW] Equipamiento Informático (Hardware), Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.[31]

7.1.6 [COM] Redes de Comunicaciones, Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.[32]

7.1.7 [Media] Soportes de información, En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.[33]

7.1.8 [AUX] Equipamiento auxiliar, En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.[34]

7.1.9 [L] Instalaciones, En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.[35]

7.1.10 [P] Personal, En este epígrafe aparecen las personas relacionadas con los sistemas de información.[36]

---

31 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
32 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
33 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
34 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
35 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
36 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

7.2 ACTIVOS DE LA INFORMACION.

Generar un inventario del equipamiento de hardware y software de la organización, identificando si son de carácter propio o pertenecen a terceros (outsorcing, proveedores).

Portatiles: Acer Aspire E15 - rojo vino, 1 unidad, propio
Servidores: Servidor Hp Proliant Ml310e Gen8, 1 unidad, propio
Equipos de escritorio: Hewlett Packard 3400MT, 4 unidades, propios

Tabla 1. Acer Aspire E15

Especificaciones	
Modelos y diseño	Acer Aspire E15 - rojo vino
Memoria	Disco duro de 500 GB
Pantalla	Panel LED con resolución HD (1.366 x 768 pí-xeles)
Multimedia	Intel HD Graphics 520, hasta 2116MB Memoria Dinamica de Video.
Procesador y memoria RAM	Intel Core i5 – 6200U 2.3 Ghz con Turbo Boost hasta 2.8 Ghz, Memoria RAM: de 4 GB
Sistema operativo y aplicaciones	Windows 10 Compatibilidad con la mayoría de aplicaciones de escritorio Skype, Correo, Personas, Tiempo, Mensajes
Controles y conexiones	WiFi 802.11 b/g/n Puerto Ethernet Puerto HDMI 2 x USB 2.0 1 x USB 3.0 Puerto VGA Bluetooth Webcam y micrófono
Autonomía	Entre cinco y siete horas

Fuente: Autor

Tabla 2. Servidor Hp Proliant Ml310e Gen8

Especificaciones	
Marca	HP
Formato	Servidor Hp Proliant Ml310e Gen8 Micro torre - 4U
Procesador	Intel Xeon Quad-Core E3-1220 / 3.1 GHz
Soporte de Procesador	Soporta hasta 1 procesador
Memoria RAM / Expansión	2GB (instalados) / 16GB (máx.) - DDR3 SDRAM - ECC - 1333 MHz - PC3-10600
Slot de expansión	2 (total) / 2 (libre) x PCIe 2.0 x8 - longitud completa, altura completa (modo x4) 1 (total) / 1 (libre) x PCIe 2.0 x16 - longitud completa, altura completa 1 (total) / 1 (libre) x PCIe 2.0 x4 - longitud media, altura completa (modo x1) 1 (total) / 0 (libre) x CPU 4 (total) / 3 (libre) x DIMM de 240 patillas
Discos incluidos	1 x 500GB - SATA-300
Capacidad de discos	2 externo 5.25" x 1/2H 4 (total) / 3 (libre) x interno 3.5" x 1/3H
Controlador de disco / RAID	SATA (SATA-300) (Smart Array B110i) RAID 0, RAID 1, RAID 10
Controlador de red	Adaptador Ethernet NC112i de 1 Gb y 2 puertos por controlador; Aplicable a todos los modelos
Fuente de poder y refrigeración	CA 120/230 V (50/60 Hz)
Sistemas operativos soportados	Microsoft Windows Server 2012 R2
Garantía	Garantía limitada - piezas y mano de obra - 1 año - in situ
Observaciones	Controlador gráfico integrado Matrox G200

Fuente: El Autor

Tabla 3. Equipo de mesa Hewlett Packard 3400MT

Especificaciones	
Formato	Microtorre
Sistema operativo Preinstalado	Windows 7 Professional original de 32 bits*
Chipset	Intel H61 Express
Procesadores	Intel Core i3 2120 3.3 Ghz
Memoria	2 GB (2 ranuras DIMM, hasta 8 GB de DDR3 SDRAM)
Unidad de disco duro	SATA de 500GB (soporta hasta 1 TB (7200 rpm))
Medios extraìbles	Unidad de DVD-ROM HP, unidad SuperMulti DVD HP
Compartimentos de expansión	Externo: 1 de 5,25 pulgadas Interno: 1 de 3,5 pulgadas
Ranuras de expansión	3 PCIe x1 1 PCIe x16 1 MiniPCI
Tarjeta grafica	Tarjeta grafica Integrada Intel HD
Audio	Tarjeta grafica Integrada Intel HD
Comunicaciones	Controlador Gigabit Ethernet integrado Realtek RTL8171
Puertos y conectores	Frontal: 2 Puertos USB 2.0, salida para audífonos y conector para micrófono Parte posterior: 4 USB, 1 DVI-D, 1 VGA, 1 RJ-45 Ethernet, 1 entrada de audio, 1 salida de audio de canal 5.1/salida de audífonos, 1 micrófono
Dispositivos de entrada	Teclado USB estandar HP, mouse USB con desplazamiento HP
Dimensiones del chasis (ancho x prof. x alt.)	36,8 x 16,5 x 38,8 cm 14,49 x 6,50 x 15,31 pulgadas
Energìa	300 W PFC activo
Garantìa limitada y servicios	1 año de garantía limitada.

Fuente: El autor

7.3 CLASIFICACION DE LOS ACTIVOS DE ACUERDO A LOS CRITERIOS DE LA INFORMACION.

Tabla 4. Tipos de activos y descripción

Tipos de Activos	Descripción
[D] Datos / Información	Base de datos del sistema contable ContaPyme, base de datos de los diseños y logotipos generados, manuales de usuario de Contapyme, Optitex, contratos de trabajo de los empleados de la organización.
[K] Claves criptográficas	Claves de acceso a equipos de cómputo, software contable.
[SW] Software	Windows 10 Home Single Language, Windows 7 Professional original de 32 bits, Microsoft Windows Server 2012 R2,(SOFTWARE DE DISEÑO OPTITEX), software de ofimática wps office 2016 versión estable 10.2.0.6020_Free_100.103, software antivirus Avast free edition.
[HW] Equipamiento Informático (Hardware)	Acer Aspire E15, Servidor Hp Proliant Ml310e Gen8, Equipos de escritorio Hewlett Packard 3400MT, 4 unidades propios.
[COM] Redes de Comunicaciones	Modem de internet, switch trendnet 8 puertos. Conectividad a internet por operador movistar.
[Media] Soportes de información	Material impreso, memorias USB, discos DVD.
[AUX] Equipamiento auxiliar	Ups StarTec 500va Interactiva
[L] Instalaciones	Instalaciones eléctricas, 6 puntos de red cableado de red categoría 6.
[P] Personal	Juan Carlos Lozada, Luis Leonardo Guzman, Carlos Andres Lozada, Pilar Manrique, Alexander Cortes, Hilda Tovar, Consuelo Martinez, Leonor Rojas

Fuente: El autor

7.4 DIMENSIONES DE LA VALORACION

Las dimensiones se usan principalmente para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión. [37]

7.4.1 De acuerdo al impacto

7.4.1.1 Criterios de valoración. Se utiliza la siguiente escala para brindar una calificación a los activos, la magnitud de riesgo e impacto sobre los mismos:

- MB: muy bajo
- B: bajo
- M: medio
- A: alto
- MA: muy alto

Tabla 5. Valoración de acuerdo al impacto

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Tomado del libro Magerit versión 3 libro III, pag 6.

37 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

7.4.1.2 Valoración de los activos. En la siguiente tabla se expone una calificación específica de los activos de acuerdo al impacto.

Tabla 6. Valoración de activos de acuerdo al impacto

ACTIVO	AMENAZA	IMPACTO
DATOS / INFORMACIÓN	Robo de información	A
	Interceptación de información	A
	Destrucción de la información	A
CLAVES CRIPTOGRÁFICAS	Robo de claves y accesos	A
SERVICIOS	Falla en servicios de comunicación	B
	Denegación del servicio	B
SOFTWARE	Caídas del sistema	B
	Fallo en los servicios de comunicación	B
	Fallas en los mantenimientos y actualizaciones	M
	Software potencialmente dañino	M
	Fallas en la configuración	M
EQUIPAMIENTO INFORMÁTICO (HARDWARE)	Perdidas de equipos	A
	Robo	A
	Fallas en suministro eléctrico	B
	Desastres naturales	A
	Errores de mantenimiento (hardware)	A
	Errores de configuración	A
	Condiciones inadecuadas de temperatura	M
REDES DE COMUNICACIONES	Errores de configuración	A
SOPORTES DE INFORMACIÓN	Disco con defectos de fabricación	B
EQUIPAMIENTO AUXILIAR	Deterioro de batería	B
INSTALACIONES	Falla en cableado de datos	M
	Fallas en red y tomas eléctricas	M
PERSONAL	Ingenieria social	A
	Accesos no autorizados	M
	Errores de los usuarios	M
	Errores del administrador	M
	Abuso en los privilegios de acceso	M
	Ingreso de información falsa	M

7.4.2 De acuerdo a las dimensiones de seguridad, dentro de este aparte se definen la disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad.

7.4.2.1 Criterios de valoración

Tabla 7. Criterios de valoración de los activos

valor		***criterio***
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: Tomado del libro Magerit versión 3 libro II, pag 19.

[D] Disponibilidad, Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].[38]

[I] Integridad, Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].[39]

[C] Confidencialidad, Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].[40]

38 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
39 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012
40 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

[A] Autenticidad, Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].[41]

[T] Trazabilidad, Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].[42]

7.4.2.2 Valoración de los activos

Tabla 8. Valoracion de las dimensiones de seguridad

Activos Esenciales	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Atención personalizada	[6]			[7]	[7]
Archivos de datos y diseños		[6]	[6]	[6]	[5]
Soportes de información	[6]	[6]	[6]		

Fuente: el autor

41 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

42 AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

8. ANALISIS DE AMENAZAS CON LA METODOLOGIA MAGERIT

La siguiente información se presenta determinando los distintos tipos de activos que se pueden ver afectados por distintos tipos de amenazas, así como una descripción de cada tipo de amenaza que se puede presentar hacia la organización.

8.1 IDENTIFICACION Y VALORACION DE AMENAZAS

AMENAZAS[43]
[N] Desastres naturales
Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.1]Fuego
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones.
Descripción: Se realizó inspección en las oficinas y lugares de trabajo, evidenciándose que no hay extintores, aumentando la posibilidad de mitigar un conato de incendio que acabe con los recursos informáticos y documentos de la organización.

[N.2]Daños por agua
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones.
Descripción: La posibilidad de una inundación destruya los recursos informáticos de la organización es baja ya que los equipos de cómputo se encuentran en un segundo piso.

[N.*] Desastres naturales
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones.
Descripción; Este tipo de eventos (tormentas eléctricas, terremotos, inundaciones, etc) se producen sin intervención humana, se cuenta con un archivador para conservar la documentación generada.

[I] De origen Industrial
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, (p 25-47). España, Madrid.

[I.5] Avería de origen físico o lógico
Tipos de activos: Aplicaciones (software), equipos informáticos (hardware), soportes de información, equipamiento auxiliar.
Descripción: fallo en el software y hardware de los equipos, se puede presentar debido a un defecto de fábrica o un desbordamiento en el funcionamiento del sistema, en los equipos de cómputo no existen restricciones para la instalación de software.

[I.6] Corte del suministro eléctrico
Tipos de activos: Equipos informáticos, soportes de información (electrónicos), equipamiento auxiliar.
Descripción: Fallo en la alimentación de energía, solo se cuenta con una fuente de respaldo para el servidor.

[I.7] Condiciones inadecuadas de temperatura o humedad
Tipos de activos: Equipos informáticos, soportes de información, equipamiento auxiliar.
Descripción: No se cuenta con áreas climatizadas, los equipos de cómputo se encuentran a temperatura ambiente, no existe ningún tipo de protección para evitar la condiciones naturales.

[I.8] Fallo de servicios de comunicaciones
Tipos de activos: Redes de comunicaciones
Descripción: Interrupción en la facultad de transmisión de datos de un punto de origen a un punto de llegada, representativamente se debe a la destrucción física de los medios de conducción o a la detención de los centros de intercambio de datos, sea por fallas técnicas, destrucción o insuficiencia para atender el trafico existente.

[I.10] Degradación de los soportes de almacenamiento de la información
Tipos de activos: Soportes de información
Descripción: Como resultado del pasar del tiempo, no existe ningún procedimiento de conservación para este tipo de degradación.

[I.11] Emanaciones electromagnéticas
Tipos de activos: Equipos informáticos (hardware), media, equipamiento auxiliar, Instalaciones.
Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información, no existe forma de aislar las ondas de radio o dispositivos electrónicos.

[E] Errores y fallos no intencionados.
Fallos no intencionales causados por las personas.

[E.1] Errores de los usuarios
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), soportes de información.
Descripción: errores humanos al momento de usar los servicios, datos, etc. Los usuarios ingresan de manera errónea datos al sistema, los cuales se pueden corregir solo parte del administrador del sistema informático.

[E.2] Errores del administrador
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información.
Descripción: Errores generados por personal con privilegios de instalación y operatividad, a la fecha no se han presentado errores en el manejo y administración del software contapyme, y optitex.

[E.4] Errores de configuración
Tipos de activos: Datos de configuración
Descripción: introducción de datos de configuración erróneos, Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc, los equipos de computo pueden estar mal configurados y/o parametrizados, no cuentan con alguna configuración especifica que impida la perdida de información.

[E.8] Difusión de software dañino
Tipos de activos: Aplicaciones (software)
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Los equipos, aunque cuentan con una versión free de antivirus, no están plenamente protegidos, no se cuenta con restricciones para la instalación de software que puedan contener software malicioso.

[E.15] Alteración accidental de la información
Tipos de activos: datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones.
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Los usuarios de la plataforma contable ingresan por error registros contables que no pertenecen a los movimientos generados.

[E.18] Destrucción de información
Tipos de activos: datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones, soportes de información, instalaciones.
Descripción: pérdida accidental de información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Toda la información se encuentra en el disco principal del servidor no se cuenta con copia de seguridad frecuente.

[E.19] Fugas de información
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones, personal (revelación).
Descripción: revelación por indiscreción. No existe a la fecha ningún manual o protocolo de seguridad de la información.

[E.20] Vulnerabilidades de los programas (software)
Tipos de activos: Aplicaciones (software)
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. A la fecha no se han encontrado fallas ni vulnerabilidades en la plataforma contable ni en la plataforma de diseño, pero los equipos son susceptibles a violación de la información.

[E.21] Errores de mantenimiento / actualización de programas (software)
Tipos de activos: aplicaciones (software)
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. La plataforma contable es actualizada por el proveedor de software de acuerdo a las actualizaciones emitidas por ellos, las actualizaciones de los sistemas operativos están programadas para que estas se ejecuten de manera automática.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Tipos de activos: Equipos informáticos (hardware), soportes electrónicos, equipamiento auxiliar
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. A la fecha no se han realizado modificaciones al hardware original de los equipos.

[E.24] Caída del sistema por agotamiento de recursos
Tipos de activos: Servicios, equipos informáticos (hardware), redes de comunicaciones
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Respecto a la plataforma contable y de diseño no se han presentado caídas del sistema por carga de trabajo.

[E.25] Robo
Tipos de activos: equipos informáticos (hardware), soportes de información, equipamiento auxiliar
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Los equipos de la organización cuentan con contraseña, los datos que se manejan no se encuentran cifrados y la información en físico no cuenta con la debida protección.

[E.28] Indisponibilidad del personal
Tipos de activos: Personal interno
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, inconformidad laboral. La frecuencia de incapacidades por enfermedad o inconformidad laboral es muy baja.

[A] Ataques intencionados
Fallos deliberados causados por las personas.
La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.
[A.3] Manipulación de los registros de actividad (log)
Tipos de activos: Registros de actividad. Actualmente no hay un manejo adecuado y responsable del log de la plataforma contable, ya que no hay un responsable directo.

[A.4] Manipulación de la configuración
Tipos de activos: Registros de actividad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Los privilegios de acceso se otorgan desde el servidor principal.

[A.5] Suplantación de la identidad del usuario
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), redes de comunicaciones.
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Actualmente no existe personal contratado de manera temporal, los privilegios de acceso a la plataforma contable se administran desde el servidor para que los usuarios puedan acceder desde sus terminales.

[A.6] Abuso de privilegios de acceso
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Los permisos de usuario son asignados de acuerdo de acuerdo al grado de responsabilidad en la operación, de esta manera los usuarios con menos privilegios no pueden modificar información sensible.

[A.7] Uso no previsto
Tipos de activos: Servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones.
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. En los equipos de cómputo son de uso personal, ya que almacenan información ajena a los propósitos de la organización.

[A.8] Difusión de software dañino
Tipos de activos: aplicaciones (software)
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. No hay software anty-spyware instalado en los equipos, de igual manera no se tiene restricción frente a la instalación de cualquier tipo de software.

[A.11] Acceso no autorizado
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones.
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Para ingresar al sistema de información se debe acceder primero al sistema operativo, posteriormente se ingresa usuario y contraseña a la plataforma contable contapyme, las modificaciones de información dependen del nivel de acceso al que este previamente autorizado.

[A.14] Interceptación de información (escucha)
Tipos de activos: Redes de comunicaciones
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. Es posible obtener información si en determinado caso llegan a conectarse por medio de la red wifi con la que se dispone ya que esta no maneja un cifrado de seguridad del más alto nivel.

[A.15] Modificación deliberada de la información
Tipos de activos: Datos / información, claves criptográficas, servicios (acceso), aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones.
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Se requiere establecer medidas de protección para asegurar la información de la organización.

[A.18] Destrucción de información
Tipos de activos: Datos / información, claves criptográficas, servicios (acceso), aplicaciones, soportes de información, instalaciones.
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Es posible instalar cualquier tipo de software sin verificar su procedencia u origen.

[A.19] Revelación de información
Tipos de activos: datos / información, claves criptográficas, servicios (acceso), aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones.
Descripción: revelación de información. No se cuenta con anti spyware instalado en los equipos y no existen mecanismos que eviten revelar la información contenida en los equipos.

[A.22] Manipulación de programas
Tipos de activos: aplicaciones (software)
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. La plataforma contable contapyme no puede ser modificada, toda modificación y/o actualización es suministrada por el proveedor del software.

[A.23] Manipulación de los equipos
Tipos de activos: Equipos, soportes de información, equipamiento auxiliar
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Los equipos se encuentran inventariados, pero cualquier modificación de hardware software debe ser autorizada por el gerente general

[A.24] Denegación de servicio
Tipos de activos: Servicios, equipos informáticos (hardware), redes de comunicaciones.
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Los servidores no han presentado problemas de sobrecarga, pero los demás equipos pueden sufrir la denegación del servicio.

[A.25] Robo
Tipos de activos: Equipos informáticos (hardware), soportes de información, equipamiento auxiliar
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.
En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. En las instalaciones se cuenta con un sistema de alarma contratado con una empresa de seguridad privada.

[A.29] Extorsión
Tipos de activos: Personal interno
Descripción: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. No existen mecanismos ni documentación que fomente las acciones preventivas frente a casos de extorsión.

[A.30] Ingeniería social (picaresca)
Tipos de activos: Personal interno
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. No se cuenta con mecanismos ni documentación dirigida a los usuarios que permitan conocer sobre el tema de ingeniería social.

Posibles vulnerabilidades en la organización: Los equipos con los que cuenta la organización tiene una alta probabilidad de tener fallas en la actualización de los antivirus instalados, de igual manera no se cuenta con un anti-spyware, solo el servidor de aplicaciones cuenta con un sistema de alimentación ininterrumpida, no se cuenta con un área especializada para el sistema informático, el servidor de aplicaciones está instalado en la gerencia, el soporte de la aplicación contable es de parte del proveedor del software. Al no contar con restricciones en los equipos de cómputo el personal puede descargar, instalar aplicaciones y guardar documentos de índole personal, de igual manera tienen acceso libre al uso de memorias usb, la documentación contable de mayor impacto es impresa y guardada en un archivador, en el momento que exista un evento vandálico o de delincuencia los equipos no poseen ningún tipo de respaldo de información.

El siguiente análisis de riesgos es realizado por medio de la metodología magerit.

8.1.1 Criterios de evaluación: los criterios de evaluación serán determinados de acuerdo a su valor, los cuales son:

MB: muy bajo
B: bajo
M: medio
A: alto
MA: muy alto

8.1.2 Evaluación de amenazas a los activos

Tabla 9. Evaluación de las amenazas a los activos

ACTIVO	AMENAZA	PROBABILIDAD
DATOS / INFORMACIÓN	Robo de información	M
	Interceptación de información	M
	Destrucción de la información	M
CLAVES CRIPTOGRÁFICAS	Robo de claves y accesos	B
SERVICIOS	Falla en servicios de comunicación	B
	Denegación del servicio	B
SOFTWARE	Caídas del sistema	B
	Fallo en los servicios de comunicación	B
	Fallas en los mantenimientos y actualizaciones	B
	Software potencialmente dañino	M
	Fallas en la configuración	M
EQUIPAMIENTO INFORMÁTICO (HARDWARE)	Perdidas de equipos	B
	Robo	A
	Fallas en suministro eléctrico	B
	Desastres naturales	MB
	Errores de mantenimiento (hardware)	B
	Errores de configuración	B
	Condiciones inadecuadas de temperatura	M
REDES DE COMUNICACIONES	Errores de configuración	M

Tabla 9. (Continuación)

ACTIVO	AMENAZA	PROBABILIDAD
SOPORTES DE INFORMACIÓN	Disco con defectos de fabricación	B
EQUIPAMIENTO AUXILIAR	Deterioro de batería	B
INSTALACIONES	Falla en cableado de datos	B
	Fallas en red y tomas eléctricas	B
PERSONAL	Ingeniería social	B
	Accesos no autorizados	MB
	Errores de los usuarios	B
	Errores del administrador	B
	Abuso en los privilegios de acceso	MB
	Ingreso de información falsa	B

Fuente: el autor

DATOS/INFORMACIÓN: La corrupción de la información es de carácter medio ya que el único que cuenta con un respaldo en caso de una falla de fluido eléctrico es el servidor de aplicaciones, brindando la posibilidad de apagar de manera correcta el servidor y evitar una perdida abrupta de información, los equipos de los usuarios no cuenta con este tipo de respaldo.

CLAVES CRIPTOGRAFICAS: la probabilidad de robo de claves y accesos es baja, la plataforma contable y de diseño son de carácter local, no poseen salida al exterior.

SERVICIOS: son casos muy poco frecuente los fallos en los servicios de la plataforma contable contapyme, el proveedor del software facilita asesoría en caso de presentarse alguna falla.

SOFTWARE: Los equipos de escritorio realizan operaciones básicas de ofimática y se accede desde ellos a la plataforma contable, por lo cual la carga de trabajo es baja, la probabilidad de tener instalado software potencialmente dañino es de carácter medio ya que no existen restricciones para la instalación de software.

EQUIPAMIENTO INFORMÁTICO (HARDWARE): Lo equipos son usados en un recinto cerrado, se cuenta con un probabilidad alta de robo por las condiciones de seguridad de la zona donde está ubicada la organización, de igual manera las condiciones de temperatura del sitio no son las más óptimas para el buen funcionamiento de los equipos.

REDES DE COMUNICACIONES: La configuración de la red local y el acceso wifi se encuentran configuradas de manera básica, sin contar con firewall o un gestor unificado de amenazas (UTM).

SOPORTES DE INFORMACIÓN: los discos dvd en los que se realizan copias de algunos archivos tiene una baja afectación por defectos de fabricación.

EQUIPAMIENTO AUXILIAR: se cuenta con una ups de respaldo para el servidor, su afectación es baja ya que solo el deterioro de la batería impediría su correcto funcionamiento.

INSTALACIONES: se deben verificar la configuración de la red cableada e inalámbrica para brindar mayores parámetros de seguridad, de igual manera se debe verificar la red eléctrica y sus respectivas toma corriente a fin que cumplan la norma RETIE.

PERSONAL: Se debe brindar capacitaciones a los empleados sobre las buenas practicas respecto a los sistemas de información y de esta manera generar conciencia y evitar eventos que atenten contra el sistema informático con el que cuenta la organización.

8.2 RIESGO POTENCIAL

8.2.1 Criterios de Evaluación

Tabla 10. Criterios de aceptación del riesgo

RANGO	DESCRIPCION
Riesgo<=M	La organización considera el riesgo poco identificable
Riesgo>M	La organización considera el riesgo identificable y se debe ejecutar su respectivo procedimiento.

8.2.2 Evaluación del riesgo potencial a los activos

Tabla 11. Análisis de riesgos

ANALISIS DE RIESGOS				
ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
DATOS / INFORMACIÓN	Robo de información	M	A	A
	Interceptación de información	M	A	A
	Destrucción de la información	M	A	A
CLAVES CRIPTOGRÁFICAS	Robo de claves y accesos	B	A	A
SERVICIOS	Falla en servicios de comunicación	B	B	B
	Denegación del servicio	B	B	B
SOFTWARE	Caídas del sistema	B	B	B
	Fallo en los servicios de comunicación	B	B	B
	Fallas en los mantenimientos y actualizaciones	B	M	M
	Software potencialmente dañino	M	M	M
	Fallas en la configuración	M	M	M
EQUIPAMIENTO INFORMÁTICO (HARDWARE)	Perdidas de equipos	B	A	A
	Robo	A	A	A
	Fallas en suministro eléctrico	B	B	B
	Desastres naturales	MB	A	M
	Errores de mantenimiento (hardware)	B	A	M
	Errores de configuración	B	A	A
	Condiciones inadecuadas de temperatura	M	M	M
REDES DE COMUNICACIONES	Errores de configuración	M	A	A
SOPORTES DE INFORMACIÓN	Disco con defectos de fabricación	B	B	B
EQUIPAMIENTO AUXILIAR	Deterioro de batería	B	B	B

Tabla 11. Continuación

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
INSTALACIONES	Falla en cableado de datos	B	M	M
	Fallas en red y tomas eléctricas	B	M	M
PERSONAL	Ingeniería social	B	A	A
	Accesos no autorizados	MB	M	B
	Errores de los usuarios	B	M	M
	Errores del administrador	B	M	B
	Abuso en los privilegios de acceso	MB	M	B
	Ingreso de información falsa	B	M	M

Fuente: el autor

9. APLICACIÓN DE CONTROLES

9.1 CONTROLES ANEXO A.

Los controles están fundamentados Anexo A del estándar ISO/IEC 27001:2013, los cuales son esenciales para poder ejecutar y/o administrar un sistema de gestión de la seguridad de la información.

Tabla 12. Anexo A del estándar ISO/IEC 27001:2013

Núm.	Nombre	Selección / excepción	Descripción / Justificación
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	X	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información	X	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	X	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	X	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	X	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles	X	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo	X	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección	X	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	X	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	X	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	X	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	X	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	X	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	X	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.8.1.2	Propiedad de los activos	X	Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	X	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	X	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información	X	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	X	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información		Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos		Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles	X	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios		Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	X	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	X	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red	X	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	X	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	X	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.9.2.4	Gestión de información de autenticación secreta de usuarios	X	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	X	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	X	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones	X	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información	X	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	X	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	X	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	X	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía		
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	X	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	X	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física	X	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.11.1.2	Controles físicos de entrada	X	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	X	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	X	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos	X	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos		Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	X	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	X	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	X	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	X	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	X	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados		Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.12.1.2	Gestión de cambios		Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	X	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo		Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información	X	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes	X	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	X	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	X	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	X	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas	X	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes	X	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	X	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información	X	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información	X	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	X	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	X	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	X	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	X	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	X	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	X	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro		Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas		Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros		Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro		Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente		Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas		Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba		Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba		Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	Relación con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	X	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	X	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	X	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	X	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	X	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos	X	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	X	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	X	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	X	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	X	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.16.1.7	Recolección de evidencia	X	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	X	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	X	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	X	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
A.17.2	Redundancias	X	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	X	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	X	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	X	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	X	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Núm.	Nombre	Selección / excepción	Descripción / Justificación
A.18.2	Revisiones de seguridad de la información	X	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información	X	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	X	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	X	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}.{03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

9.2 POLITICAS DE SEGURIDAD

9.2.1 POLITICAS GENERALES

- Cada usuario que realice algún tipo de labor en algún equipo de cómputo debe ingresar con usuarios y contraseña.

- Los usuarios solo deben tener acceso a los servicios asignados y autorizados.

- El acceso a internet se debe realizar de manera cautelosa, en el momento que se realicen actividades laborales, Evitar realizar descargas de software o apliciones de origen desconocido.

- Durante el uso del correo electrónico de los colaboradores evitar abrir mensajes de remitentes desconocidos.

- Los usuarios deben realizar un uso adecuado de los equipos de computo, de igual manera informar a la gerencia sobre cualquier falla, desperfecto o alguna eventualidad que impida el desarrollo de las actividades.

- Las contraseñas contendrán al menos 3 de las siguientes condiciones: números, letras mayúsculas, letras minúsculas, símbolos; además poseer tenga mínimo 8 caracteres de longitud.

- El acceso a la gerencia, sitio donde se encuentra el servidor de aplicaciones se encuentra totalmente restringido, solo se autoriza el ingreso al personal designado por el gerente para las labores que sean requeridas.

- Se debe mantener el escritorio del computador (Windows) totalmente limpio de información confidencial para la organización.

- En caso de que el trabajador se retire de su puesto de trabajo, debe bloquear inmediatamente la sesión activa.

- Se debe usar un protector de pantalla ante inactividad del equipo de computo, el mismo que se establecerá para activarse luego de 2 minutos de inactividad.

- Todos los archivos creados por los usurios deben ser almacenados en la carpeta “Mis Documentos”, a fin de poder agilizar el procedimiento alinstante de realizar copias de seguridad.

- Los usuarios son directamente responsables de sus usuarios y contraseñas, por tal motivo deben prescindir de compartir y/o difundir sus datos de acceso de las sesiones de Windows o software que utilizen.

9.2.2 POLITICAS DE SEGURIDAD A NIVEL FÍSICO

- Todos los trabajadores deben contar con un carnet institucional, con el fin de poder realizar la respectiva identificación

- Se deberá contar con un sistema de detección de intrusos a efectos de controlar el acceso físico en horas no laborables.

- Se deberá mantener extintores contra fuego cerca del cuarto donde se encuentran el servidor y el archivo físico, se debe revisar anualmente para su respectivo mantenimiento.

- Con el objetivo de proteger los activos de información físicos, se prohíbe el consumo de comidas y bebidas en los escritorios de trabajo donde se encuentren equipos de computación y/o documentos físicos.

- Se prohíbe el consumo de cigarrillos dentro de las áreas de trabajo de la oficina.

- Se destina el área de recepción como punto de entrega y carga. El acceso a las oficinas estará condicionado a los trabajadores bajo previa autorización. Si un proveedor necesita ingresar para entregar suministros debe ser acompañado por un funcionario de la organización.

9.2.3 POLITICAS DE SEGURIDAD A NIVEL LÓGICO.

- Todo equipo con sistema operativo Windows debe tener activo el firewall de comunicaciones para evitar infección y posibles ataques al computador.

- Todos los equipos con sistema operativo Windows debe tener instalado un software antivirus, el cual se actualizara de manera automatica, igualmente se realizara una revisión cada treinta (30) dias, que incluya la actualización general de la base de datos de firma de virus, análisis del equipo en busca de amenazas, eliminación de amenazas encontradas.

- Los equipos que cuentan con puertos USB y acceso a unidades CD/DVD, están bajo responsabilidad del usuario al cual esta asignado, asi como el ingreso y salida de información.

- Los usuarios que están autorizados para el uso de dispositivos de almacenamiento externo estan en la obligacion de hacer uso del antivirus antes de ejecutar cualquier tipo de acción a fin de evitar que los equipos sean infectados.

- Todo archivo de dudosa procedencia debe ser rechazado.

- No usar contraseñas semejantes para el ingreso a sistemas abiertos, como por ejemplo: correo electrónico, foros, etc., a las que usa para la administración o acceso a equipos de la empresa.

- No conectarse de ninguna manera a redes inalámbricas de dudosa procedencia, si se va a manejar información de carácter confidencial.

- Las contraseñas contendrán al menos 3 de las siguientes condiciones: números, letras mayúsculas, letras minúsculas, símbolos; además poseer tenga mínimo 8 caracteres de longitud.

- Al finalizar cada trimeste del año se realizara cambio de contraseña para el acceso a las sesiones de Windows como a los programas que se usan en la organización.

9.2.4 POLITICAS DE RESPALDO Y RECUPERACION DE INFORMACIÓN

- Las copias de respaldo de la información se realizara una vez al dia previo a finalizar la jornada laboral.

- Mediante una aplicación se realizara la copia correspondiente y se almacenara en un disco externo.

- Se deben realizar pruebas de restauración, al menos una vez al año.

9.2.5 POLITICAS DE MANTENIMIENTO DE EQUIPOS

- Antes de encender el equipo de computo asegurarse de que este cuenta con las condiciones de ambiente adecuadas.

- Al finalizar la jornada laboral se debe apagar el equipo de computo ejecutando la opción “Apagar” y esperar hasta que el proceso concluya debidamente.

- Evitar manipular la pantalla de los computadores o laptops con los dedos, uñas u otro objeto.

- Cuando el equipo portatil se encuentre cerrado evitar colocar carpetas o elementos encima del mismo.

- Evitar el consumo de comidas y bebidas en los puestos de trabajo donde se encuentren equipos de cómputo o documentación.

- El equipo deber estar ubicado y resguardado para reducir los riesgos de las amenazas y las oportunidades para el acceso no autorizado.

- Se deberá contar con protección ante fallas o interrupciones de energía mediante la utilización de UPS, en caso de una interrupción de energía se

debe realizar apagado de los equipos de cómputo para evitar perdidas de información.

- Se debe verificar que las ups funcionen de manera idónea y estén en optimas condiciones de uso, de no ser asi se debe realizar mantenimiento preventivo o correctivo ya sea el caso.

- Se debe realizar mantenimiento preventivo físico a los equipos de computo, estos se realizaran cada 4 meses por personal capacitado.

- Los mantenimientos preventivos físicos programados a los equipos de cómputo, se realizaran dentro de las instalaciones de la organización y bajo supervisión de una persona asignada por la gerencia.

- Toda actividad de mantenimiento realizada por el personal de sistemas contratado deberá estar documentada a fin de hacerle el seguimiento respectivo.

9.2.6 POLITICAS DE USO DE SOFTWARE

- Todos los equipos deben contar con las últimas actualizaciones del sistema operativo Windows y parches de seguridad.

- Está prohibido el uso de programas sin licencias no autorizadas por la empresa.

- Los usuarios no deben instalar o intentar instalar programas, utilitarios o complementos para navegadores de internet. Esta actividad está reservada solo al personal de sistemas contratado por la organización.

9.3 RECOMENDACIONES

La concientización de la organizacion respecto al tema de seguridad informática es un punto clave y fundamental, por lo cual la organización debe poner mucho empeño en despertar el interés y compromiso de todos sus empleados, la prevención y la anticipación son las mejores herramientas.

Realizar inversión de una herramienta antivirus con licencia Premium para garantizar la seguridad de la información en los equipos de computo, de esta

manera tendremos disponibles actualizaciones y contaremos con la máxima protección contra diversas amenazas.

Las consultorias por parte de especialistas en seguridad informática darán a conocer diversas características en esta temática y aportaran conocimientos en la prevención respecto a la instalación de programas que vulneren la privacidad de la información.

La creación de manuales de confidencialidad de la información, brindaran apoyo a la organización ante el suministro no adecuado de algún tipo de declaración o comunicación a personas ajenas a la organización.

Brindar capacitaciones frecuentes al personal sobre las buenas practicas y uso de las herramientas informáticas, de esta manera se crea conciencia en el personal y se evitan fugas de información de manera inconciente.

Contar con sistemas de respaldo de información (backups) permiten a la organización tener accesibilidad a la misma en un momento determinado,esta practica es de gran uso y en caso de fallas del sistema de información nos permite recuperar información en un lapso de tiempo preestablecido.

Implementar medidas de seguridad que sean aplicables en caso de robo de equipos o extorsion, permiten a la compañía asegurar los equipos de computo y documentación que comprometa las actividades propias de su objeto social.

Se recomienda instalar sistemas de alimentación ininterrumpida (ups) en cada uno de los equipos de cómputo de la organización, de esta manera se garantiza la vida útil de los equipos de computo, la conservación adecuada de los sistemas informáticos y los documentos que se generan en el mismo.

10. CONCLUSIONES

Se hallan distintas fallas de seguridad en la organización, igualmente la ausencia de capacitación en cada uno de los empleados es evidente, los activos se deben cuidar en un lugar adecuado y con las condiciones de ambiente adecuadas para evitar su deterioro, el descenso en los riesgos obtendrá como resultado la disponibilidad, confiabilidad e integridad de la información.

Es necesario instaurar manuales de seguridad para los distintos casos que se presenten en los posibles eventos de una fuga de información, la gerencia debe contar con ellos en caso de una posible auditoria y de esta manera generar seguridad y determinación en los empleados al momento de realizar actividades que impliquen el uso de recursos informáticos.

Se realiza el análisis de las deficiencias encontradas en la organización, se hace extensiva la invitación a la gerencia de la organización para que hagan la implemnetacion de un SGS, ya que al momento solo se ha conformado la identificación de las amenazas, riesgos y vulnerabilidades, pero los controles y recomendaciones deben ser tomadas en cuenta a fin de obtener un mejoramiento en el estándar de calidad como empresa y propender por ser una organización líder en el mercado.

Es necesario hacer énfasis que la implementación de un SGSI es un compromiso de mejoramiento continuo, lo anterior a fin de tomar las medidas necesarias para el funcionamiento adecuado y optimo de la organización.

BIBLIOGRAFIA

Wikipedia. la enciclopedia libre. Activo (contabilidad), {En linea}. {01 de mayo de 2018} disponible en: (https://es.wikipedia.org/wiki/Activo_(contabilidad))

Departamento de seguridad informática. Amenazas a la Seguridad de la Información. Universidad Nacionalde Luján, Luján, Buenos Aires, Argentina. {En linea}. {01 de mayo de 2018} Disponible en: (http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12)

Ecured. Conocimiento con todos y para todos. Sistema Informatico. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.ecured.cu/Sistema_inform%C3%A1tico)

CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En linea}. {01 de mayo de 2018}. Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

Ronquillo, Sixto. Controles en la seguridad de la información. {En linea}. {01 de mayo de 2018} disponible en : (https://prezi.com/gkwjvmaeivtc/controles-en-la-seguridad-de-la-informacion/)

Fisher, Dennis. Kaspersky Lab Daily. ¿Qué es un botnet?. {En linea}. {01 de mayo de 2018} Disponible en : (https://www.kaspersky.es/blog/que-es-un-botnet/755/)

Ecured. Conocimiento con todos y para todos. Ciberespacio. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.ecured.cu/Ciberespacio)

Ciberdefensa-Ciberseguridad Riesgos y Amenazas, {En linea}. {01 de mayo de 2018}, Disponible en : (http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf)

Wikipedia. la enciclopedia libre. Magerit (metodología). {En linea}. {01 de mayo de 2018} Disponible en : (https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa))

Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

Seguridad Informatica. Objetivos de la seguridad informática. {En linea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

Wikipedia. la enciclopedia libre. Politica de seguridad. {En linea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad)

Arbelaez, Ana. Ingenieria social: El hackeo silencioso. {En linea}. {02 de mayo de 2018} Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

Wikipedia. la enciclopedia libre. Sistema de gestión de la seguridad de la información. {En linea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n)

CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En linea}. {01 de mayo de 2018} Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

Gobierno Digital. Enterate. MinTIC desarrolla el Modelo Nacional de Riesgos y genera capacidades humanas en Seguridad Digital, {En linea}. {03 de mayo de 2018} Disponible en: (http://estrategia.gobiernoenlinea.gov.co/623/w3-article-61852.html)

Contapyme NIIF. ContaPyme® Software administrativo y contable para pymes. Que es contapyme? {En linea}. {03 de mayo de 2018} Disponible en: (https://www.contapyme.com/software-contable/)

Gestion. Las Normas Internacionales de Información Financiera (NIIF). {En linea}. {03 de mayo de 2018} Disponible en : (https://gestion.pe/tendencias/normas-internacionales-informacion-financiera-niif-51948)

El costurero de stella. Que esoptitex?. {En linea}. {03 de mayo de 2018} Disponible en: (https://www.elcosturerodestellablog.com/2009/03/que-es-optitex.html)

ANGARITA VIVAS, Alexis Armando. TABARES ISAZA, Cesar Augusto. Análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de pereira s.a e.s.p, basados en la norma iso 27005. Pereira, 2012, 104p. Proyecto de Grado para optar por el título de

Especialista en Redes de Datos. Universidad tecnológica de Pereira. facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación.

GARCIA HERNANDEZ, David Alejandro. RUIZ MURILLO, Jeisson Herley, analisis y gestion de riesgos en el marco del sgsi, basado enla metodologia magerit y apoyado en un api web para su ejecucion. Bogota, 2017, 225p. Monografía de grado para ingeniería telemática. Universidad distrital francisco josé de caldas. Facultad tecnológica ingenieria en telemática.

Investigación Holistica. La investigación proyectiva. {En linea}. {03 de mayo de 2018} Disponible en: (http://investigacionholistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html)

Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009. {En linea}. {03 de mayo de 2018} Disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

Ministerio de Tecnologías de la Información y las Comunicaciones. normativa del gobierno electrónico en Colombia. {En linea}. {03 de mayo de 2018} Disponible en: (http://viejoprograma.gobiernoenlinea.gov.co/apc-aa-files/5686d2a87532a21a70ead773ed71353b/NormativaGEL.pdf)

Alcaldia Mayor de Bogota. Regimen Legal de Bogota D.C. Ley 1266 de 2008 Nivel Nacional. {En linea}. {03 de mayo de 2018} Disponible en : (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488)

AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, (p 25-47). España, Madrid.

Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}. {03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

ANEXOS

Anexo A. Politica general de la seguridad de la información.

En la empresa textil diseños y dotaciones Osiris S.A.S la información es un activo esencial para el desarrollo de sus actividades comerciales, asi como la toma de decisiones. Motivo por el cual existe un convenio para la protección de sus activos mas representativos, siendo pieza fundamental en la estrategia de continuidad del negocio.

Como un acto consecuente a las necesidades de diseños y dotaciones Osiris S.A.S, implementa un modelo de gestión de seguridad de la información como instrumento que permita determinar, analizar y disminuir los riesgos a los que se encuentra expuesto la información, impulsando la disminución de costos admiistrativos y operativos, la socialización e implementación de una cultura enfatizada en la seguridad garantiza el cumplimiento de los requisitos legales, contractuales y regulatorios vigentes a la fecha.

Todos los funcionarios, personal ajeno a la organización y todo individuo que posea un compromiso sobre las fuentes de información, documentación y recursos informáticos de diseños y dotaciones Osiris S.A.S, deberán acoger los parámetros expuestos en el siguiente documento y todos aquellos que contenagn un vinculo con el, con el propósito de conservar la integridad, confidencialidad y garantizar la disponibilidad de la información.

Anexo B. Sanciones a las violaciones de las políticas de seguridad de la información

Las políticas de seguridad de la información procuran establecer y consolidar la educación en cuanto a la seguridad de la información en la organización, dando alcance a los funcionarios, personal ajeno a la organización y todo individuo que tenga algún tipo de relación con diseños y dotaciones Osiris S.A.S, por tal motivo es necesario que las violaciones a las políticas de seguridad de la información se encuentran debidamente catalogadas, con el fin de poder aplicar las medidas correctivas de conformidad con la clasificación previamente definida y asi disminuir las eventuales afectaciones contra la seguridad de la información. Las medidas de índole correctivo están consideradas desde acciones de orden administrativo hasta acciones de orden disciplinario y/o penal, tomando referencia las circunstancias acontecidas.

Anexo C. Politica para uso de dispositivos móviles

Diseños y dotaciones Osiris S.A.S establecera las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smartphones”, tabletas), entre otros, tanto corporativos como personales y que hagan uso de los servicios de los servicios de información de la organización, de igual manera se inspeccionara que el personal haga un uso adecuado y consciente de los servicios que la organización pone a disposición.

La gerencia deberá determinar que tipo de configuraciones son aceptables tanto para los dispostivos móviles empresariales como personales que hagan uso de los servicos dispuestos por la empresa.

La gerencia autoriza el uso de WhatsApp únicamente en dispositivos que estén conectados a los servicios dispuestos por la organización, no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

La gerencia debe verificar que los dispositivos móviles que hagan uso de los servicios de la organización deben contar con software antivirus, a fin de evitar la propagación de cualquier tipo de virus.

Es responsabilidad del usuario hacer buen uso del dispositivo móvil con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.

Los usuarios de dispositivos móviles, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

Los usuarios de dispositivos móviles NO deben hacer uso de redes inalámbricas públicas.

Esta prohibido la instalación de aplicaciones en cualquier dispositivo móvil mientras este se encuentre conectado a la red wifi de la organización, caso contrario este será autorizado por la gerencia y solo se se instalaran aplicaciones de origen conocido que estén previamente autorizadas, verificadas y distribuidas desde los sitios oficiales de descarga

Anexo D. Politica de seguridad para el recurso humano

Diseños y dotaciones Osiris S.A.S, considera que el recurso humano es de vital importancia para cumplir con los objetivos corporativos y con el propósito de obtener un personal calificado y con altas competencias laborales, respaldara la vinculación de nuevo personal realizando un proceso de selección acorde a la lesgilacion vigente, el cual se orientara a los distintos roles que puedan desempeñar.

Se debe asegurar que los empleados de diseños y dotaciones Osiris S.A.S, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información

Los aspirantes y proveedores deben dar aprobación a diseños y dotaciones Osiris S.A.S para el tratamiento de sus datos personales de acuerdo a la Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

La gerencia deberá verificar la competencia necesaria de los candidatos o aspirantes a ocupar la vacante disponible.

La gerencia debe verificar la existencia de acuerdos y/o clausulas de confidencialidad, asi como la aceptación de las políticas de seguridad de la información para el personal provisto por terceros, previo al acceso a la información de diseños y dotaciones Osiris S.A.S.

A la firma del contrato laboral el empleado debe firmar un acuerdo de confidencialidad para con diseños y dotaciones Osiris S.A.S.

Se debe capacitar y sensibilizar a los empleados durante la inducción sobre las políticas de seguridad de la información.

La gerencia debe precisar y decretar el proceso disciplinario a seguir en caso de presentarse incumplimiento a las políticas de seguridad o incidentes que se llegasen a presentar.

Anexo E. Politica de uso de los activos

Diseños y dotaciones Osiris S.A.S debe brindar y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los activos de información pertenecen a diseños y dotaciones Osiris S.A. y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

Diseños y dotaciones Osiris S.A.S proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de diseños y dotaciones Osiris S.A.S, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la organización, serán sancionadas de acuerdo con las normas y legislación vigentes.

Periódicamente, la gerencia a través de un contratista profesional en sistemas efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las políticas de seguridad de la Información de diseños y dotaciones Osiris S.A.S.

Los recursos informáticos diseños y dotaciones Osiris S.A.S. no podrán ser utilizados, sin previa autorización escrita, para divulgar, promover o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los usuarios no deben realizar de manera intencional acciones que impliquen un uso inadeacuado de los recursos tecnológicos o que vayan en resistencia de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, utilización de juegos en línea, uso permanente de redes sociales personales, etc.

Los usuarios no podrán ejecutar ninguna de las siguientes acciones sin previa autorización de la gerencia:

- Instalar software en cualquier equipo de computo de diseños y dotaciones Osiris S.A.S.
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de computo de diseños y dotaciones Osiris S.A.S.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de diseños y dotaciones Osiris S.A.S.
- Copiar o distribuir cualquier software de propiedad de diseños y dotaciones Osiris S.A.S..
- Cambiar la configuración de hardware de propiedad de diseños y dotaciones Osiris S.A.S.

El usuario será responsable de todas las transacciones o acciones ejecutadas con su “cuenta de usuario”.

Toda unidad de almacenamiento externa, deberá ser revisada para detección de virus y otros programas maliciosos antes de ser instalados en los equipos de cómputo de diseños y dotaciones Osiris S.A.S.

Todos los archivos provenientes de equipos ajenos a diseños y dotaciones Osiris S.A.S., deben ser revisados para detección de virus antes de su utilización dentro de la red y equipos de computo de la organización.

La información de diseños y dotaciones Osiris S.A.S. debe ser respaldada de forma frecuente, debe ser almacenada en un lugar apropiado en el cual se pueda garantizar que la información este segura y esta podra ser recuperada en caso de un desastre o incidentes con los equipos de computo de la organización.

Anexo F. Politica de acceso a redes y recursos de red

La gerencia de diseños y dotaciones Osiris S.A.S, como administrador de la red de datos y recursos de red de la organización, debe garantizar que las redes de datos se encuentren debidamente aseguradas contra accesos no autorizados.

La gerencia debe garantizar que la red inalámbrica de la organización cuente con los mecanismos de autenticación paraevitar accesos no autorizados.

Los equipos de cómputo asignados a los usuarios que se encuentren conectados a las redes de datos de la organización deben contar con todas las condiciones y controles para acreditarse en ellas y solo podrán ejecutar las tareas para las que fueron asignados.

La gerencia debe instaurar un método de autorización y control para resguardar el acceso a las redes de datos y los recursos de red de diseños y dotaciones Osiris S.A.S.

La gerencia debe instaurar los respectivo controles para la identificación y autenticación de todos los usuarios, ya sean internos o externos y que hagan uso de las redes o recursos de red de diseños y dotaciones Osiris S.A.S, igualmente velar por el consentimiento de los compromisos de adquiridos por los usuarios, igualmente es necesario precisar la aceptación de las políticas de seguridad de la información por parte de cada uno de ellos.

Todos los usuarios sin excepción alguna al referir ingreso por primera vez a la red de datos de diseños y dotaciones Osiris S.A.S, deben diligenciar con el formato de creación de cuentas de usuario previamente autorizado, anexando el acuerdo de confidencialidad debidamente firmado.

La gerencia verificara periódicamente los controles de acceso de todos los usuarios a fin de garantizar que el acceso a los recursos de red y servicios sean aquellos a los que previamente fueron autorizados.

Anexo G. Resumen Analitico Especializado – RAE

Fecha de Realización: 15 de abril de 2018
Titulo: ANALISIS Y GESTION DE RIESGOS AL SISTEMA DE INFORMACION DE LA EMPRESA TEXTIL DISEÑOS Y DOTACIONES OSIRIS S.A.S APLICANDO METODOLOGIA MAGERIT
Autor: Jiménez Urbano, Giovanny Ernesto
Palabras Claves: Amenazas, sistema informático, vulnerabilidades, activos informáticos, controles.
Descripción: Monografia de estudio sobre la implementación de la metodología MAGERIT analizando los riesgos y vulnerabilidades, presentando políticas de seguridad para el mejoramiento continuo de los estándares de seguridad de la información en la empresa textil diseños y dotaciones Osiris S.A.S.
Fuentes: Wikipedia. la enciclopedia libre. Activo (contabilidad), {En linea}. {01 de mayo de 2018} disponible en: (https://es.wikipedia.org/wiki/Activo_(contabilidad)). Departamento de seguridad informática. Amenazas a la Seguridad de la Información. Universidad Nacionalde Luján, Luján, Buenos Aires, Argentina. {En línea}. {01 de mayo de 2018} Disponible en: (http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12). Ecured. Conocimiento con todos y para todos. Sistema Informatico. {En línea}. {01 de mayo de 2018}. Disponible en: (https://www.ecured.cu/Sistema_inform%C3%A1tico) CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En línea}. {01 de mayo de 2018}. Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo) Ronquillo, Sixto. Controles en la seguridad de la información. {En línea}. {01 de mayo de 2018}, disponible en : (https://prezi.com/gkwjvmaeivtc/controles-en-la-seguridad-de-la-informacion/) Fisher, Dennis. Kaspersky Lab Daily. ¿Qué es un botnet?. {En línea}. {01 de mayo de 2018}. Disponible en : (https://www.kaspersky.es/blog/que-es-un-botnet/755/)

Ecured. Conocimiento con todos y para todos. Ciberespacio. {En línea}. {01 de mayo de 2018}. Disponible en: (https://www.ecured.cu/Ciberespacio)

Ciberdefensa-Ciberseguridad Riesgos y Amenazas, {En línea}. {01 de mayo de 2018} Disponible en : (http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf)

Wikipedia. la enciclopedia libre. Magerit (metodología). {En línea}. {01 de mayo de 2018} Disponible en : (https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa))

Seguridad Informatica. Objetivos de la seguridad informática. {En línea}. {01 de mayo de 2018} Disponible en (https://infosegur.wordpress.com/tag/disponibilidad/)

Seguridad Informatica. Objetivos de la seguridad informática. {En línea}. {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

Seguridad Informatica. Objetivos de la seguridad informática. {En línea} {01 de mayo de 2018} Disponible en : (https://infosegur.wordpress.com/tag/disponibilidad/)

Wikipedia. la enciclopedia libre. Politica de seguridad. {En línea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad)

Arbelaez, Ana. Ingenieria social: El hackeo silencioso. {En línea}. {02 de mayo de 2018}. Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

Wikipedia. la enciclopedia libre. Sistema de gestión de la seguridad de la información. {En línea}. {02 de mayo de 2018} Disponible en: (https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n)

CODEJOBS. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En línea}. {01 de mayo de 2018}. Disponible en: (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo).

Gobierno Digital. Enterate. MinTIC desarrolla el Modelo Nacional de Riesgos y genera capacidades humanas en Seguridad Digital, {En línea}. {03 de mayo de 2018}. Disponible en: (http://estrategia.gobiernoenlinea.gov.co/623/w3-article-61852.html)

Contapyme NIIF. ContaPyme® Software administrativo y contable para pymes. Que es contapyme? {En línea}. {03 de mayo de 2018}. Disponible en: (https://www.contapyme.com/software-contable/)

Gestion. Las Normas Internacionales de Información Financiera (NIIF). {En línea}. {03 de mayo de 2018}. Disponible en : (https://gestion.pe/tendencias/normas-internacionales-informacion-financiera-niif-51948)

El costurero de stella. Que es optitex?. {En línea}. {03 de mayo de 2018} Disponible en: (https://www.elcosturerodestellablog.com/2009/03/que-es-optitex.html)

ANGARITA VIVAS, Alexis Armando. TABARES ISAZA, Cesar Augusto. Análisis de riesgos para el proceso administrativo: departamento de informática en la empresa de acueducto y alcantarillado de pereira s.a e.s.p, basados en la norma iso 27005. Pereira, 2012, 104p. Proyecto de Grado para optar por el título de Especialista en Redes de Datos. Universidad tecnológica de Pereira. facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación.

GARCIA HERNANDEZ, David Alejandro. RUIZ MURILLO, Jeisson Herley, analisis y gestion de riesgos en el marco del sgsi, basado enla metodologia magerit y apoyado en un api web para su ejecucion. Bogota, 2017, 225p. Monografía de grado para ingeniería telemática. Universidad distrital francisco josé de caldas. Facultad tecnológica ingenieria en telemática.

Investigación Holistica. La investigación proyectiva. {En línea}. {03 de mayo de 2018} Disponible en: (http://investigacionholistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html)

Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009. {En línea}. {03 de mayo de 2018} Disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

Ministerio de Tecnologías de la Información y las Comunicaciones. normativa del gobierno electrónico en Colombia. {En línea}. {03 de mayo de 2018} Disponible en: (http://viejoprograma.gobiernoenlinea.gov.co/apc-aa-files/5686d2a87532a21a70ead773ed71353b/NormativaGEL.pdf)

Alcaldia Mayor de Bogota. Regimen Legal de Bogota D.C. Ley 1266 de 2008 Nivel Nacional. {En línea}. {03 de mayo de 2018}. Disponible en : (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488)

AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012

AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, (p 25-47). España, Madrid.

Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. {En linea}. {03 de mayo de 2018}. Disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

Contenido del documento:

La metodología MAGERIT

Metodologia:

Este tipo de investigación, consiste en la elaboración de una propuesta, un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo.

El origen de la información es adquirida directamente de los empleados de la empresa textil diseños y dotaciones osiris s.a.s, se constituyen como objetivos:

Identificar el grado de vulnerabilidad de la red de datos frente a ciberataques, mediante revisión del estado actual de su sistema de información, identificar los activos de información que son propiedad de diseños y dotaciones Osiris S.A.S, determinar los riesgos y amenazas de los activos de información que son propiedad de diseños y dotaciones Osiris S.A.S, plantear controles basados en la norma ISO27000:2013 a los riesgos identificados en diseños y dotaciones Osiris S.A.S, elaborar el informe gerencial con los resultados obtenidos durante el análisis de riesgos y divulgación de las recomendaciones de seguridad sugeridas para la organización diseños y dotaciones Osiris S.A.S, proyectar políticas de seguridad, con base a los distintos controles sugeridos.

Conceptos Nuevos:
Metodologia MAGERIT, Norma ISO 27001, amenazas, riesgos, vulnerabilidades, controles, políticas de seguridad.

Conclusiones:
Se hallan distintas fallas de seguridad en la organización, igualmente la ausencia de capacitación en cada uno de los empleados es evidente, los activos se deben cuidar en un lugar adecuado y con las condiciones de ambiente adecuadas para evitar su deterioro, el descenso en los riesgos obtendrá como resultado la disponibilidad, confiabilidad e integridad de la información.

Es necesario instaurar manuales de seguridad para los distintos casos que se presenten en los posibles eventos de una fuga de información, la gerencia debe contar con ellos en caso de una posible auditoria y de esta manera generar seguridad y determinación en los empleados al momento de realizar actividades que impliquen el uso de recursos informáticos.

Se realiza el análisis de las deficiencias encontradas en la organización, se hace extensiva la invitación a la gerencia de la organización para que hagan la implemnetacion de un SGS, ya que al momento solo se ha conformado la identificación de las amenazas, riesgos y vulnerabilidades, pero los controles y recomendaciones deben ser tomadas en cuenta a fin de obtener un mejoramiento en el estándar de calidad como empresa y propender por ser una organización líder en el mercado.

Es necesario hacer énfasis que la implementación de un SGSI es un compromiso de mejoramiento continuo, lo anterior a fin de tomar las medidas necesarias para el funcionamiento adecuado y optimo de la organización.

Autor:
GIOVANNY ERNESTO JIMENEZ URBANO