DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ALGORÍTMICOS M&C

LUIS MANUEL MESA MENDIVELSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL, COLOMBIA
2020

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ALGORÍTMICOS M&C

LUIS MANUEL MESA MENDIVELSO

EDGAR MAURICIO LOPEZ ROJAS
Director De Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL, COLOMBIA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Yopal, Agosto 2020

AGRADECIMIENTOS

Mi sincero agradecimiento a todas aquellas personas que hicieron posible el desarrollo de éste proyecto, contando siempre con el apoyo académico de la UNAD (Universidad Abierta y a Distancia) y a Yeny Sirley Dueñas, quien permitido llevar a cabo en su organización el SGSI.

CONTENIDO

Pag

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

Actualmente, en un mundo globalizado, donde prima el crecimiento tecnológico, las entidades buscando ser más competitivas, fortalecen metodologías operativas, para lograr procesos más eficientes y flujo de datos efectivos, por ello, la información generada en el transcurso de sus actividades, paso a ser un Activo de gran valor, en consecuencia, es fundamental adoptar medidas para asegurarlo y protegerlo, mitigando riesgos a nivel estructural e individual dentro de la organización, puesto que, sin importar su tamaño, es igual de vulnerable.

Para salvaguardar de manera eficaz dicho Activo, la Organización Internacional de Normalización (ISO), asegura que toda empresa puede obtener Certificación ISO 27001, una norma diseñada para gestionar de forma segura la información, la cual se caracteriza por ser aplicable en cualquier tipo de empresa.

En ésta síntesis, mediante un desarrollo contextual, se da a conocer el diseño de un Sistema de Gestión de Seguridad de la Información, para la empresa Algoritmos M & C, basado en la Norma Internacional ISO 27001, mediante recolección de información, inventario de activos, análisis de riesgos, identificaciones de vulnerabilidades y amenazas, para establecer controles y políticas de seguridad, las cuales brindan recomendaciones y acciones, permitiendo mostrar un panorama general en cuanto a su seguridad informática limitado a procesos generales de la empresa que estén documentados.

1. DEFINICION DEL PROBLEMA

Actualmente, la entidad Algoritmos M & C, no ha desarrollado controles y políticas que garanticen seguridad informática, la información en cada uno de sus departamentos, está propensa a su eliminación o secuestro por entes externos, evidenciando también, una posible pérdida de la misma a gran escala.

Por ello, es necesario proponer y diseñar un sistema de gestión para la seguridad de la información, cuya función sea garantizar que los riesgos expuestos anteriormente sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios en el flujo o manejo diario de la información.

Para diseñar un Sistema de Gestión de Seguridad de la Información, se toma como referencia la Norma Internacional ISO 27001, la cual nos permite garantizar protección, disponibilidad e integridad de datos, tanto de manera interna, como externa, así, se podrá prevenir riesgos y detectar todo problema que afecte y dañe la información en la entidad Algoritmos M & C.

La confidencialidad implica el acceso a la información por parte únicamente de quienes están autorizados, así mismo, la integridad conlleva el mantenimiento exacto y completo de la información, junto a sus métodos de procesos permitiendo disponibilidad a la información y los sistemas de tratamiento por parte de los usuarios facultados en el momento que lo requieran.

El estándar ISO 27001, busca disminuir de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal.

Para proteger a la organización Algoritmos M & C de todas estas amenazas, es necesario conocerlas y afrontarlas de una manera adecuada. Para ello debemos establecer unos procedimientos adecuados y diseñar controles de seguridad basados en la evaluación de riesgos y su eficacia.

¿Cómo mediante el diseño un Sistema de Gestión de Seguridad de la Información se logrará disminuir los riesgos y la inseguridad de la información en la empresa Algorítmicos M&C?

2. OBJETIVOS

2.1. Objetivo general.

- Diseñar un sistema de gestión de Seguridad de la Información, en la empresa ALGORITMICOS M&C, bajo los lineamientos del Estándar Internacional ISO 27001 para seguridad de la información.

2.2. Objetivos específicos

- Ejecutar una revisión del estado actual de la seguridad de la Información en la empresa Algorítmicos M&C.
- Realizar análisis y evaluación de las vulnerabilidades, mediante la matriz de riesgos.
- Gestionar los riesgos encontrados mediante la aplicación de controles, tomando como referencia la norma ISO 27001

3. JUSTIFICACIÓN

La mayoría de las organizaciones modernas sin importar su tamaño, recopilan, procesan o transmiten datos a través de sus diferentes activos informáticos. La información en formato digital cada día juega un papel más esencial en la toma de decisiones para alcanzar los objetivos organizacionales, sin embargo, está sujeta a amenazas constantes de tipo natural o humano; para las organizaciones es esencial protegerla, así como los activos informáticos, mediante actividades y procesos coordinados que permitan mantener su confidencialidad, integridad y disponibilidad. Estas actividades y procesos son gestionados de forma clara y concisa por medio de un Sistema de Gestión de la Seguridad de la Información donde el estándar ISO 27001, es uno de los más reconocidos a nivel internacional y propone un ciclo de mejoramiento continuo para la empresa Algorítmicos M&C.

Algorítmicos M & C en sus procesos y servicios telemáticos ofertados en la región se ve en la necesidad de garantizar, salvaguardar y proteger los activos informáticos e información crítica y sensible donde la exposición más cercana se contempla con el diseño de un Sistema de Gestión de Seguridad de la Información, como lo recomienda la norma ISO 27001, la cual permitirá que se emplee prácticas adecuadas de seguridad de la información y a su vez concientizando a sus empleados sobre los riesgos y amenazas actuales a través de prácticas, procedimientos, guías y lineamientos documentados y liderados por la alta gerencia.

Como los sistemas de gestión son procesos en mejoramiento continuo, la fase de diseño o planeación es la piedra angular, ya que define los lineamientos sobre los cuales se regirán las demás fases determinando el alcance, políticas y objetivos generales, por consiguiente, la fase de diseño será el punto de partida para una posterior implementación del Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO 27001, mitigando así los riesgos potenciales sobre los activos informáticos en la organización.

4. ALCANCE Y LIMITACIONES

El presente proyecto comprende la fase de diseño de un sistema de gestión de la seguridad de la información, con el objetivo de cumplir los requerimientos establecidos por los controles y procedimientos necesarios para el mejoramiento continuo de la empresa.

Durante el diseño del sistema de gestión de la seguridad de la información se planifica y diseñan controles logrando establecer políticas de seguridad de la información.

Para elaborar un plan de implementación de un sistema de gestión de la seguridad de la información es necesario la autorización y aprobación para el diseño y/o ejecución al propietario de la empresa, si el propietario no está de acuerdo, inmediatamente se verán reducidos los alcances y se tendrá que reformular el plan de implementación.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

Ley 1273 de 2009.

Los tres pilares fundamentales de la seguridad informática son: la confidencialidad, la integridad y la disponibilidad; por lo tanto, para preservar estos principios, el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273, por medio de la cual, se modifica el Código Penal y se crea un nuevo bien jurídico tutelado, denominado: “De la Protección de la información y de los datos”, que pretende proteger la información, los datos y la preservación integral de los sistemas que utilicen tecnologías de la información y las comunicaciones.

Ésta ley, es de gran importancia como un apoyo legal para proteger la información de las organizaciones o personas naturales, propensas en igualdad a éstos problemas. Además, conocer dicha ley, posibilita un mecanismo de respuesta rápido para defender su activo más importante como lo es la información.

Proceso de Administración del Riesgo en Seguridad de la Información

El proceso o ciclo de manejo en seguridad de la información se fundamenta en cinco fases o macro actividades, que se muestran a continuación, cuyo fin último, es mantener los riesgos en el manejo de la información de la organización en un nivel tolerable.

A continuación, en la siguiente figura se puede evidenciar el ciclo de la seguridad de la información:

Fig. Ciclo Seguridad De La Información

Fuente: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Administración del Riesgo en Seguridad de la Información

Este ciclo se lleva a cabo mediante la ejecución rigurosa y secuencial de cinco actividades:

Evaluar el Riesgo: El proceso de administración del riesgo en seguridad de la información inicia por establecer que debe ser protegido, para lo que se identifica el valor de la información del negocio y los riesgos a que está expuesta cuantificados en su impacto; y en general se realiza un diagnóstico que pretende establecer un nivel de seguridad comparado con las mejores prácticas. Dicho valor de referencia le permitirá a la organización establecer hitos con sus respectivas fechas en el logro de niveles de seguridad de la información aceptables por el negocio.

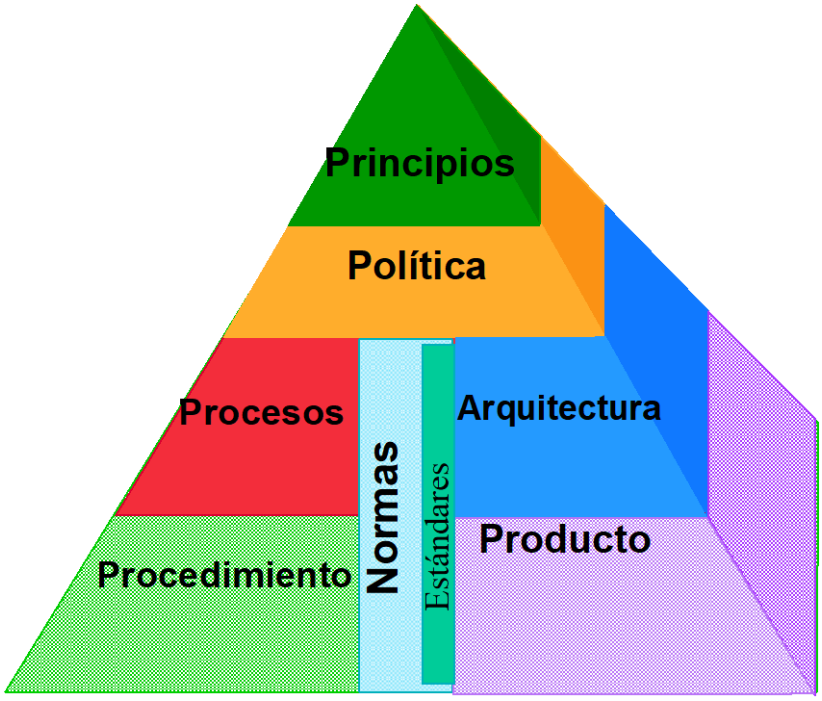
Diseño: Una vez se ha identificado la información crítica y los riesgos a que está expuesta se diseña la manera como deben ser protegida, para lo que se desarrolla la Política de Seguridad de la Información, basada en los principios organizacionales.

Ésta Política es el fundamento de la seguridad de la información y es la directriz para el desarrollo de acciones que permitan su cumplimiento, como las normas, los procesos y procedimientos, la arquitectura de seguridad y los productos de seguridad de la información; grupo más conocido como Modelo de Seguridad.

El desarrollo de un Modelo de Seguridad de la información es una iniciativa en la que se aglutinan múltiples acciones, que permiten desplegar la Política de

Seguridad a lo largo y ancho de una Institución y lograr los niveles de seguridad aceptados por el negocio. Sus principales componentes, como se muestra en la figura son:

Figura 1. Modelo de la seguridad de la información.



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Modelo de Seguridad de la Información

- Los principios de Seguridad son proposiciones de valor requeridas por una institución para llevar a cabo un adecuado manejo de riesgo en seguridad de la información, que le permitan lograr las metas del negocio a un nivel aceptable de riesgo.

- Las Política de Seguridad de la información, son proposiciones de alto nivel compuesta de objetivos, fines, creencias, ética y responsabilidades en la administración del riesgo en seguridad de la información.

- Las Normas de Seguridad de la información, son un conjunto de reglas para implantar la Política.

- Los Estándares de Seguridad en tecnología informática, son un conjunto de reglas detalladas, que hacen mención específica de tecnologías, metodologías, procedimientos de implantación, y otros factores, resultantes de aplicar la norma.

- Los Procesos de Seguridad de la información, son una serie de actividades y tareas típicamente realizadas a través de varias organizaciones para implantar las políticas y normas.

- Los procedimientos de Seguridad de la información, son los pasos operacionales específicos que las personas deben ejecutar para alcanzar los objetivos establecidos en las políticas.

- La arquitectura de Seguridad en la tecnología informática, son los detalles de cómo la tecnología se relaciona y se junta para lograr los objetivos de la Política.

- Los productos de Seguridad son el conjunto de herramientas ofrecidas por la organización de Seguridad de la información, que permitirán implantar los servicios de seguridad encargados de mantener el riesgo a niveles aceptables.

6 DISEÑO METODOLÓGICO

7.1. METODOLOGÍA

Para éste proyecto, se implementa un enfoque metodología - analítico, ya que, permite descomponer el todo del problema en partes o elementos más pequeños, con el fin de conocer la causas de su origen, puesto que, se necesita conocer la naturaleza del problema para poderlo entender , junto con la metodología inductiva, la cual complemente en forma adecuada a la práctica, debido a sus componentes esenciales que conllevan cuatro pasos: observación, clasificación, derivación inductiva y contrastación; con la finalidad de brindar hipótesis aplicables a la obtención de una solución del problema.

Los pasos a seguir serán tomados de la siguiente manera:

6.1.2 Recolección de la información: Se recopiladora la información la información de la empresa mediante inventario de activos, encuestas y cuestionarios personalizados según perfiles de los colaboradores.

6.1.3 Muestras: Como muestra al ser una pequeña empresa inferior a 10 colaboradores, tomaremos el 100% de los empleados.

6.1.4 PROCESAMIENTO DE LA INFORMACIÓN

La información recolectada se analizará y clasificará para identificar amenazas, vulnerabilidad y riesgos con el objetivo de elaborar controles y una política de seguridad.

6.1.4.1 Metodología para el análisis y diseño. Se buscará procesos que permitirán elaborar controles con el objetivo de mitigar dichos riesgos y vulnerabilidades identificadas

6.5.1 ESTABLECER EL SGSI

6.5.1.1 Alcance. Con el fin de mejorar la calidad en la prestación del servicio Algorítmicos se aplica el SGSI a los procesos, recursos informáticos y tecnológicos que hacen parte del área de informática de la empresa con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información y debe ser aplicada y cumplida por todos los empleados de la organización.

6.5.1.2 Política del Sistema de Gestión. Algorítmicos pretende que la información manejada por sus usuarios y clientes esté debidamente protegida con el fin de

preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información, ya que es una entidad privada encargada de prestar servicios telemáticos.
El gerente es el responsable de la implementación de los requerimientos de seguridad con el fin de proteger la información por lo tanto en su organización se debe elaborar un análisis y evaluación del riesgo para gestionarlos adecuadamente y disminuir eventos indeseados.

6.5.1.3 Metodología de Evaluación del Riesgo.
Se realizaron los siguientes pasos para la evaluación de los riesgos

1: Inventario de Activos
2: Valoración de los activos
3: Amenazas (identificación y valoración)
4: Salvaguardias
5: Impacto y riesgo residuales
Resultados del análisis de riesgos

6.6 Análisis de Riesgos de la empresa Algorítmicos

6.6.1 Inventario de Activos. Las empresas deben proteger la confidencialidad, integridad y disponibilidad de la información para velar por la continuidad del negocio independientemente de su actividad social. Para proteger dicha información de riesgos y amenazas Algorítmicos realiza un inventario de sus activos teniendo en cuenta nuestra metodología.

7 RESULTADOS

7.1 Estado actual y levantamiento de la información de la empresa

Descripción de los activos en la empresa Algorítmicos

A continuación, se relación los activos de la empresa

Tabla 1 Activos Algoritmicos

ACTIVOS ALGORITMICOS		
Tipo Activo	**Descripcion**	**Observacion**
Datos Digitales	Personales	Hojas de vida colaboradores
	Legales	Contratos y ordenes de servicios
	Bases de datos	Toda la informacion de la empresa y sus contratistas
	Copias de seguridad	Respaldo de la informacion de Algoritmicos.
Hardware IT	Dispositivos de almacenamiento	Discos duros, memorias USB - Dispositivos de respaldos -Contingencias
	Modem	Modem suministra internet - Proveedor CLARO
	Servidor	Equipo Mesa Lenovo, procesador I5, Disco duro 1 TB, Ram 4, S.O Centos Version 6.9
	Equipo Escritorio	HP todo en uno,Procesador I3, disco duro 500 Gb, Ram 4, Windows 10
	Portatil	HP Pavilion DV5 procesador i5, Disco duro 1 Tb, Ram 8, windows 10
Servicios IT	Webmin	Administracion grafica de los servicios en el servidor Centos
	Servicio Proxy	Squid, servicio instalado en S.O Centos
	Servicio Backup	Amanda, servicio para realizar copias de seguridad en Centos
	Servicio Telnet	Servicio instalado en los equipos clientes para interactuar con el servidor
	Servicio Escritorio Remoto	VNC, servicio instalado en centos para acceder remotamente al servidor.
	Servicio Web	Apache, servicio instalado en centos como servidor web.
	Servicio FTP	Servicio instlaado en Centos para la descarga de archivos de gran tamaño.
Aplicaciones	MobaXterm 12.3	Aplicación Free cliente Telnet y SSH para windows
	VNC Client	Aplicacion Free cliente para tomar acceso remoto al servidor para windows
	7 - Zip 18.05	Aplicacion Free para gestionar archivos comprimidos
	NotePad ++ 7.8	Aplicacion Free editor de codigo fuente para windows
	Java 7 72	Aplicacion Free complemento y plugin para el buen funcionaminto de aplicaciones en windows
	FileZilla Client 3.11	Aplicacion free cliente para interacturar con el servidor
	Office 365 Hogar	Licencia con cobertura para 6 equipos.
	Xampp Server 7.2	Aplicacion Free para gestionar bases de datos y sitios web de manera local para windows
	Acrobat Reader DC	Aplicacion Free para visualizar archivos pdf en windows
	Avast	Aplicacion Free antivirus limitado teniendo en cuenta su version gratuita para windows

Fuente: El autor

7.2 Valoración cualitativa de los activos. Teniendo en cuenta que todos los activos no tienen la misma relevancia e importancia para la empresa y que cada uno de estos en caso de ser atacado o sufrir un incidente genera un impacto diferente en

la organización, se procede a realizar una valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo con la siguiente Tabla.

Tabla 2 Criterios de Valoración

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: El autor

7.7.1 Valoración Cualitativa de Activos esenciales

En la siguiente tabla se procede a relacionar los activos esenciales de la empresa

Tabla 3 Valoración Cualitativa de Activos esenciales

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[vr]	Datos vitales	[I_Proyectos]	Información de Proyectos radicados (base de datos y registro de proyectos)	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
		[I_Licencias]	Información de Licencias	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	
		[I_Normativa]	Información de Normativa (Normas locales, nacionales, POT, acuerdos, decretos, Cartografía)	Confiabilidad	
				Integridad	3
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	
[per]	Datos de Carácter Personal	[I_Contabilidad]	Contabilidad de la empresa	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[classified]	Datos clasificados	[E_S_Licenciador]	Ejecutable software Licenciador	Confiabilidad	
				Integridad	6
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	
		[D_Históricos]	Datos Históricos de proyectos radicados	Confiabilidad	3
				Integridad	3
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[D_Proyectos]	Documentación de proyectos tramitados.	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	

Fuente: El autor

7.7.2 Valoración Cualitativa de Datos/Información

En la siguiente tabla se relaciona la valoración a los activos tipificados como datos e información

Tabla 4 Valoración Cualitativa de Datos/Información

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[files]	Ficheros	[A_proyectos]	Archivos de proyectos radicados	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Clientes]	Archivos de Clientes	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Contabilidad]	Archivo de Contabilidad	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Informes y Licencias]	Archivos de Informes y licencias expedidas	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Confiabilidad	
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos radicados	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de empleados	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

Fuente: El autor

7.7.4 Valoración Cualitativa de Servicios. Los servicios son para los clientes y empleados.
A continuación, se describe la valoración de los servicios de la empresa

Tabla 5 Valoración Cualitativa de Servicios

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los empleados.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónicos	Confiabilidad	6
				Integridad	6
				Autenticidad	7

Fuente: El autor

7.7.5 Valoración Cualitativa de Software – Aplicaciones Informáticas.
En la siguiente tabla se evidencia la valoración de los aplicativos de la empresa

Tabla 6 Valoración Cualitativa de Software

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
[Oficce]	Ofimática	[Oficce]	Office 2010	Confiabilidad	

Fuente: El autor

7.7.6 Valoración Cualitativa de Equipos Informáticos

A continuación, se relaciona la valoración de los equipos informáticos de la empresa

Tabla 7 Valoración Cualitativa de Equipos Informáticos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[S_Aplicaciones]	Servidor Aplicaciones Servidor de Base de Datos Servidor Aplicaciones Servidor de Base de Datos Servidor Aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	
		[S_Database]	Servidor de Base de Datos	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	
[mid]	Equipos medios (Equipos de trabajo	[PC_trabajadores]	Equipos de mesa	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	

Fuente: El autor

7.7.7 Valoración Cualitativa de Redes de comunicaciones

En la siguiente tabla se relación la valoración de los equipos de comunicación de la empresa

Tabla 8 Valoración Cualitativa de Redes de comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	
[LAN]	Red local	[R_Local]	[LAN]	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	
[Internet]	Internet	[Internet]	[Internet]	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	

Fuente: El autor

7.7.8 Valoración Cualitativa de Soportes de Información _almacenamiento electrónico

A continuación, se procede a relacionar los resultados de la valoración

Tabla 9 Valoración Cualitativa de Soportes de Información _almacenamiento electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	
[cd]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
[USB]	Memorias	[A_Memorias]	Almacenamiento en Memorias	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	

Fuente: El autor

7.7.9 Valoración Cualitativa de Soportes de Información _almacenamiento no electrónico

En la siguiente tabla se relaciona la valoración de la información no digital de la empresa

Tabla 10 Valoración Cualitativa de Soportes de Información _almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Material impreso	C_ Documentación proyecto	Carpetas con la documentación de cada proyecto(documentación, planos, memorias de cálculo y estudios de suelos)	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		C_ Reportes e informes	Carpetas de reportes e informes impresos	Confiabilidad	
				Integridad	7

Fuente: El autor

6. Identificación de Amenazas. La valoración de amenazas se realiza teniendo en cuenta la frecuencia con la que ocurre, las dimensiones de seguridad y la escala de rango porcentual de impactos en los activos

A continuación, se evidencia la escala de rangos de frecuencias de amenazas

Tabla 11 Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: El autor

En la siguiente tabla se relaciona las dimensiones de la seguridad a valorar

Tabla 12 Dimensiones de seguridad

Dimensiones de Seguridad a valorar	Identificación
Autenticidad	A
Confiabilidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: El autor

Escala de rango porcentual de impactos en los activos para cada dimensión de la seguridad

Tabla 13 Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: El autor

En la siguiente tabla se procede a identificar las amenazas para el inventario de activos realizado. En algunos casos se toma los activos más críticos o la categoría, identificando su frecuencia e impacto.

Tabla 14 Relación Amenaza por activo, Frecuencia – Impacto

Relacion de amenaza por activo identificando su frecuencia e impacto								
Amenaza	Activo		Frecuencia de la amenaza	Impacto para cada Dimension de seguridad (%)				
				[A]	[C]	[I]	[D]	[T]
Manejo inadecuado de datos críticos	Datos Digitales	Personales	5	20	75		5	
		Legales	5			75		
Transmisión no cifrada de datos críticos		Bases de datos	10			75	100	
		Copias de seguridad	10		75		100	
Infección de sistemas a través de unidades portables	Hardware IT	Dispositivos de almacenamiento	100			5		
		Modem	70		20			
Falta de mantenimiento físico		Servidor	10				100	
Perdida de datos por error de hardware		Equipo Escritorio	70					20
		Portatil	70				20	5
Falta de actualización de software	Servicios IT	Webmin	5				75	
		Servicio Proxy	5				20	
Falla de software - corrupción		Servicio Backup	10	50			100	
Fuga Informacion		Servicio Telnet	5				5	
		Servicio Escritorio Remoto	5				20	
Falta de actualización de software		Servicio Web	5				75	
		Servicio FTP	5			75	75	

Fuente: El autor

7.2 Salvaguardas

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en este caso se tiene en cuenta las salvaguardas

Tabla 15 Tipos de salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente El Autor

7.3 Salvaguardas de Activos esenciales

Tabla 16 Salvaguardas de Activos esenciales

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[vr]	Datos vitales	[I_Proyectos]	Información de Proyectos radicados (base de datos y registro de proyectos)	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información – Acceso restringido
				Recuperación (RC)	Copias de Seguridad (por lo menos dos respaldos guardados en sitios seguros)
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[I_Licencias]	Información de Licencias	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Recuperación (RC)	Copias de Seguridad de los archivos de licencias
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas

Fuente: El autor

7.4 Salvaguardas de Datos/Información

Tabla 17 Salvaguardas de Datos/Información

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[files]	Ficheros	[A_proyectos]	Archivos de proyectos radicados	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[A_Clientes]	Archivos de Clientes	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[A_Contabilidad]	Archivo de Contabilidad	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios

Fuente: El autor

7.1 Salvaguardas de Servicios

Tabla 18 Salvaguardas de Servicios

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)	Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad

Fuente: El autor

7.2 Salvaguardas de Software – Aplicaciones Informáticas

Tabla 19 Salvaguardas de Software – Aplicaciones Informáticas

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el	Detección (DC)	Activación de IDS y Firewall, software de monitorización y escaneo,

Fuente: El autor

7.3 Salvaguardas de Equipos Informáticos

Tabla 20 Salvaguardas de Equipos Informáticos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[S_Aplicaciones]	Servidor Aplicaciones	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Monitorización(Mn)	Registro de descarga, registro de acceso
				Detección (DC)	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus
				Concienciación (AW)	Capacitación al personal en el manejo.
		[S_Database]	Servidor de Base de Datos	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Eliminación (EL)	Eliminación de cuentas sin

Fuente: El autor

7.4 Salvaguardas de comunicaciones

Tabla 21 Salvaguardas de comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes

Fuente: El autor

7.5 Salvaguardas de Soportes de Información almacenamiento electrónico

Tabla 22 Salvaguardas de Soportes de Información almacenamiento electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
[cd]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD	Preventivas(PR)	Políticas de seguridad para

Fuente: El autor

7.6 Salvaguardas de Soportes de Información almacenamiento no electrónico

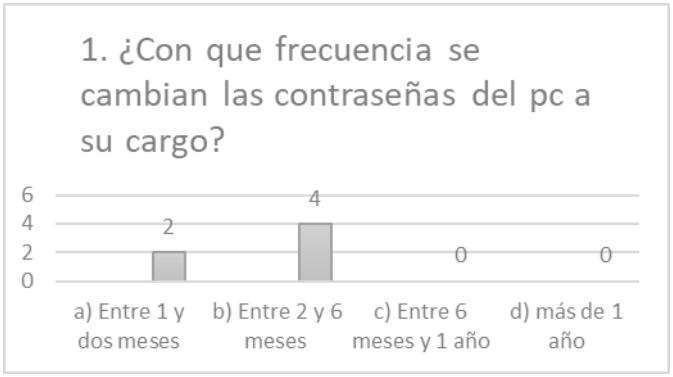
Tabla 23 Salvaguardas de Soportes de Información almacenamiento no

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[printed]	Material impreso	C_Documentaci ónproyecto	Carpetas con la documentació n de cada proyecto(docu mentación, planos, memorias de cálculo y estudios de suelos)	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
		C_Reporteseinf ormes	Carpetas de reportes e informes impresos	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
		C_Sop0rtesCont abilidad	Carpetas facturas y soportes contabilidad	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.

electrónico Fuente: El autor

Estado actual en seguridad de la información en la empresa de Algorítmicos realizada mediante una en cuesta a sus colabores arrojo lo siguiente.

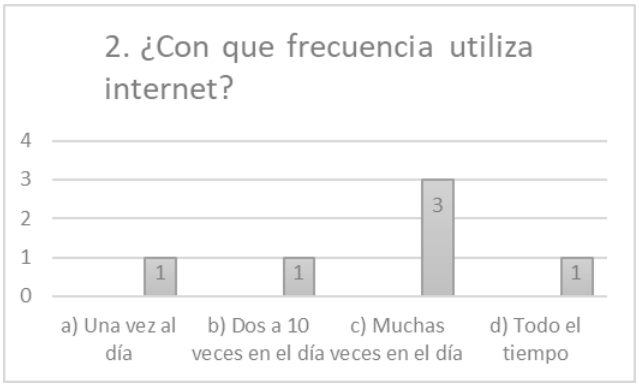
Grafica 1 Encuesta primera pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

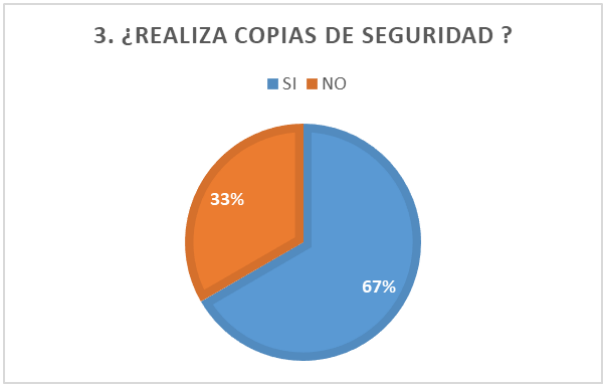
Grafica 2 Encuesta segunda pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

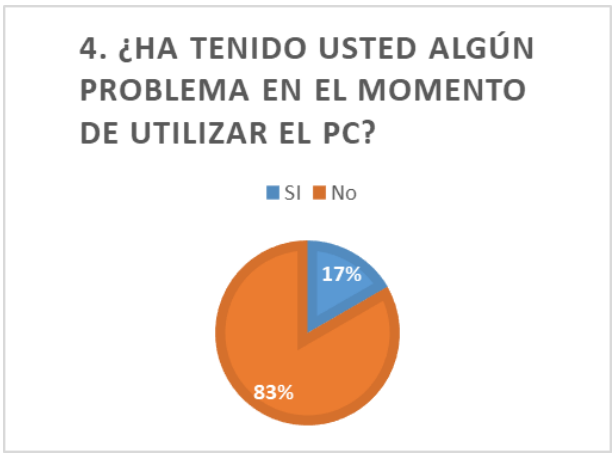
Grafica 3 Encuesta tercera pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

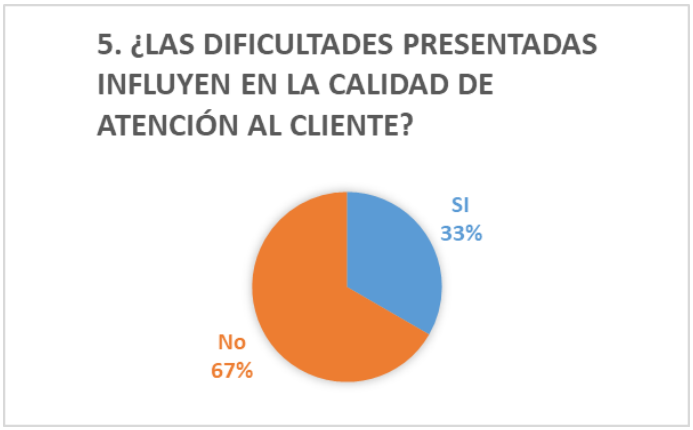
Grafica 4 Encuesta cuarta pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

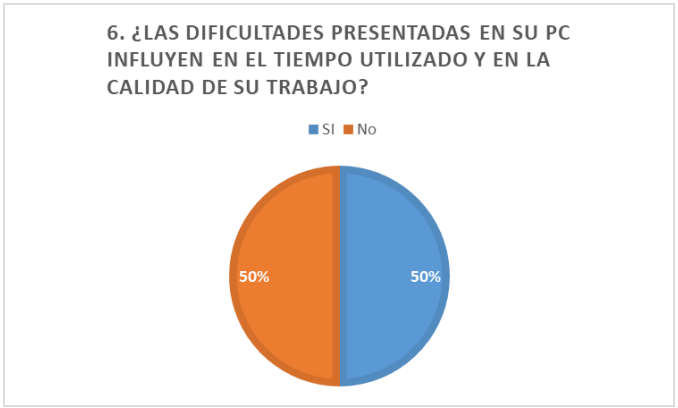
Grafica 5 Encuesta quinta pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

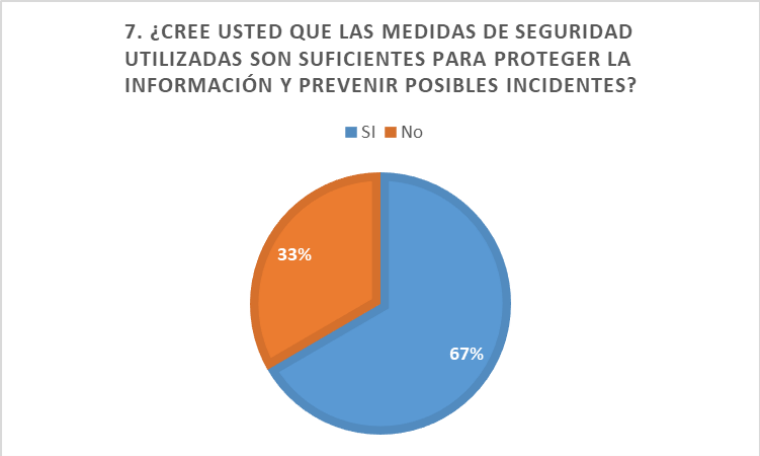
Grafica 6 Encuesta sexta pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

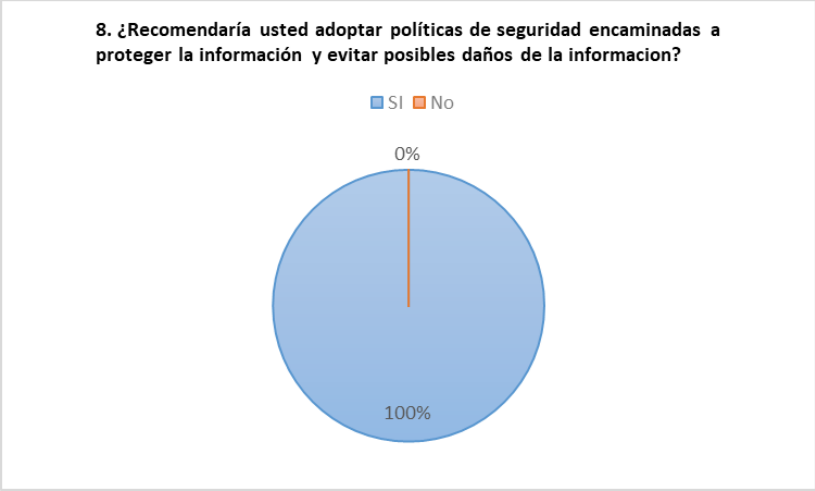
Grafica 7 Encuesta séptima pregunta



Fuente: El autor

Resultado encuesta realizado a los colabores.

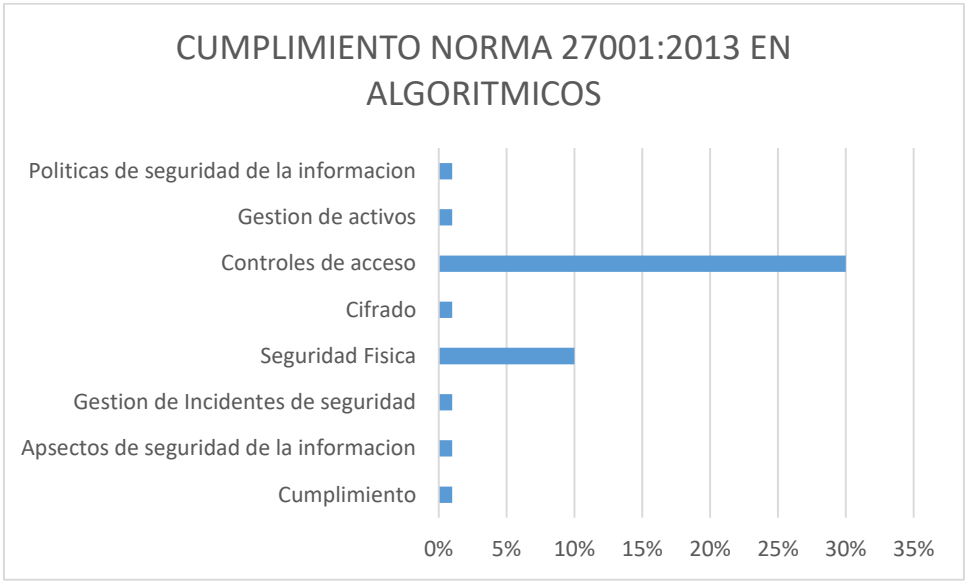
Grafica 8 Encuesta octava pregunta



Fuente: El autor

El análisis se realizó con el fin de verificar el cumplimiento de la empresa Algorítmicos frente a los controles definidos en el anexo A de la norma 27001:2013, en el cual se obtuvo lo siguiente:

Figura 2 Análisis SGSI Algorítmicos

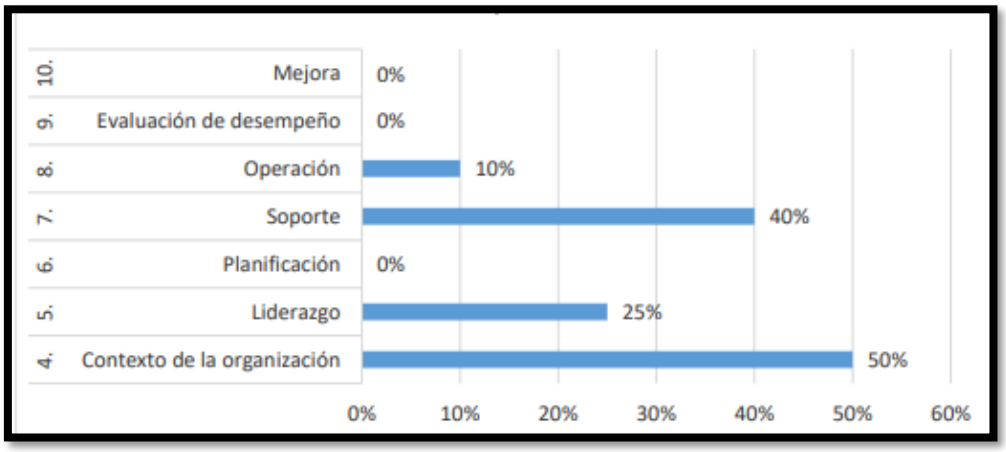


Fuente: El Autor

La empresa Algorítmicos M & C, no cumple con el estándar de la norma 27001:2013, no se evidencio controles y salvaguardas establecidos en cada proceso y rol, donde los dominios de control que presentan menor cumplimiento son: política de seguridad de la información 0%, Cifrado con el 0%, Gestión de activos 0%, Cumplimiento 0%, Gestión de incidentes de seguridad 0%.

La empresa Algorítmicos cuenta con el 5% de cumplimiento a los requisitos establecidos en la norma 27001:2013.

Figura 3 Análisis Requisitos norma 27001_2013



Fuente: El autor

8.2. Definición del alcance del SGSI

Realizar la parte de planificación estableciendo el sistema de gestión de seguridad de la información (SGSI) y la ejecución, la cual abarca la implementación y gestión

del SGSI realizando pruebas para poder verificar los resultados antes de implementarlo.
Durante todo el SGSI en la empresa se tendrán en cuenta la confidencialidad de la información las falencias y problemas para no afectar la confianza que le tiene a la empresa
Se hará el plan de implementación y se pedirá la autorización para la ejecución al dueño de la empresa, si el dueño no autoriza alguna acción se verán reducidos los alcances y se tendrá que reformular el plan de implementación.

8.3.1.1 Identificación de los riesgos derivados del acceso de terceros.

Identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.

8.3.1.2 Tratamiento de la seguridad en la relación con los clientes.

Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.

8.3.1.3 Tratamiento de la seguridad en contratos con terceros.

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.

8.4.2 Gestión de activos.

8.4.2.1 Responsabilidad sobre los activos.

8.4.2.2 Inventario de activos.
Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes

8.4.2.3 Propiedad de los activos.
Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

8.4.2.4 Uso aceptable de los activos.

Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

8.4.3 SEGURIDAD FÍSICA Y DEL ENTORNO.

8.4.3.1 Áreas seguras.

8.4.3.2 Perímetro de seguridad física.
Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.

8.4.3.4 Controles físicos de entrada.
Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.

8.4.3.5 Seguridad de oficinas, despachos e instalaciones.
Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

8.4.3.6 Protección contra las amenazas externas y de origen ambiental.
Se debería designar y aplicar medidas de protección física contra catástrofes y fenómenos naturales o de carácter humano.

8.4.3.7 Áreas de acceso público y de carga y descarga.
Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.

8.4.4 Seguridad de los equipos.

8.4.4.1 Emplazamiento y protección de equipos.
El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.

8.4.4.2 Instalaciones de suministro.
Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.

8.4.4.3 Seguridad del cableado.

Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.

8.4.4.4 Mantenimiento de los equipos.
Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.

8.4.4.5 Seguridad de los equipos fuera de las instalaciones.
Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.

8.4.4.6 Reutilización o retirada segura de equipos.
Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.

8.4.4.7 Retirada de materiales propiedad de la empresa.
No deberían sacarse equipos, información o software fuera del local sin una autorización.

8.4.5 Protección contra el código malicioso

8.4.5.1 Controles contra el código malicioso.
Se deberían ejecutar controles y políticas de seguridad para prevenir la implantación de código y software malicioso, a su vez capacitar al personal para lograr su identificación.

8.4.6 Copias de seguridad.

8.4.6.1 Copias de seguridad de la información.
Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.

8.4.7 Gestión de la seguridad de las redes.

8.4.7.1 Controles de red.
Se debe controlar el acceso limitado a la red para evitar el uso indebido y fuga de información.

8.4.8 Control De Acceso.

8.4.8.1 Requisitos de negocio para el control de acceso.

8.4.8.2 Política de control de acceso.
Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

8.4.9 Gestión de acceso de usuario.

8.4.9.1 Registro de usuario.
Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.

8.4.9.2 Gestión de privilegios.
Se debería restringir y controlar la asignación y uso de los privilegios.

8.4.9.3 Gestión de contraseñas de usuario.
Se debe implementar un mecanismo para la creación de contraseñas fuertes y robustas.

8.4.10 Responsabilidades de usuario.

8.4.10.1 Uso de contraseñas.
Se implementar una política de seguridad y concientización sobre el manejo de contraseñas.

8.4.11 Control de acceso a la red.

8.4.11.1 Control de encaminamiento (routing) de red.
En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.
8.4.12 Control de acceso al sistema operativo.

8.4.12.1 Procedimientos seguros de inicio de sesión.
Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión.

8.4.13 Control de acceso a las aplicaciones y a la información.

8.4.13.1 Restricción del acceso a la información.
Se debe perfilar y segmentar la información, es decir establecer niveles de acceso a la seguridad.

8.4.13.2 Aislamiento de sistemas sensibles.
Los sistemas sensibles deberían disponer de un entorno informático dedicado (propio).

8.4.14 Seguridad de los archivos de sistema.

8.4.14.1 Control de acceso al código fuente de los programas.
Se debería restringir y limitar el acceso al código fuente sobre todo el desarrollo de software.

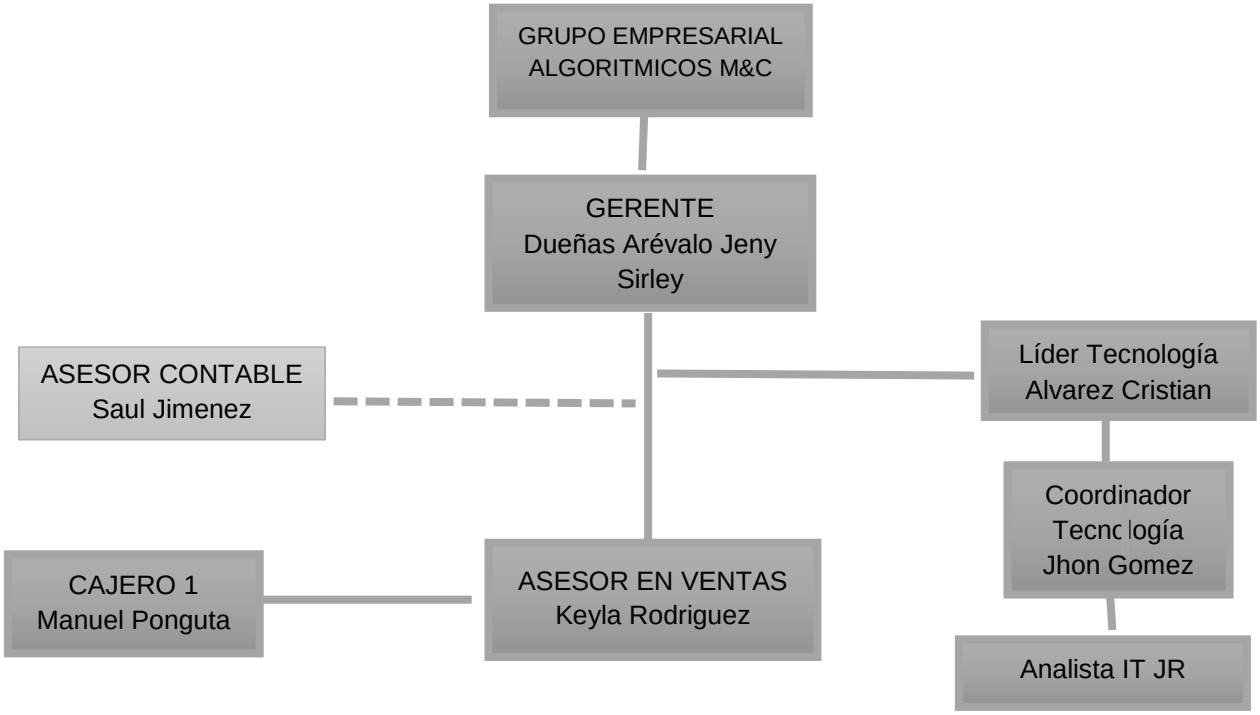
Información de la empresa y propietario de la empresa

ALGORITMICOS M&C: una pequeña empresa constituida desde año 2010, dedicada a los servicios IT en la región de Casanare.

Propietaria de la empresa: Jeny Sirley Dueñas Arévalo C.C; 1.118.554.286
Dirección; Calle 26ª #31b - 08
Municipio: Yopal – Casanare

8.3.1 ORGANIGRAMA

Figura 4 Organigrama Algoritmicos



Fuente: El Autor

Actividad principal: Actividades de telecomunicaciones alámbricas

Actividad secundaria: Comercio al por menor de equipos tecnológicos, periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados

Total, de activos: $ 6,300,000.00

Información del responsable por el SGSI: LUIS MANUEL MESA MENDIVELSO

8.4 ACTIVOS DE INFORMACIÓN

La empresa ALGORITMICOS M&C cuenta con la totalidad de la información en medios magnéticos y físicos.

La información está contenida en el servidor principal y se realizan las copias de seguridad semanalmente.

La información es la siguiente:

- Formatos y plantillas de operación.
- Desarrollo de Software
- Registros de los productos tecnológicos.

8.4.1 Valoración del riesgo de la información

Si se llegara a perder esta información por alguna condición interna u externa la empresa cuenta con la implementación de copias de seguridad garantizando la totalidad de la información.

8.5 IDENTIFICACIÓN DEL ESTADO ACTUAL EN LA EMPRESA

- La empresa no cuenta con políticas de seguridad
- La empresa cuenta con 7 empleados
- La empresa tiene acuerdos de confidencialidad respecto a la información que maneja sus empleados.

- El cableado y los computadores no están protegidos contra eventualidades climáticas, el cableado y los computadores están muy cerca del suelo
- Los equipos IT no están protegidos contra posibles robos u otras eventualidades, no existen pólizas.
- Las personas autorizadas para usar el computador donde se aloja la información principal son 2.
- Todos los computadores cuentan con ups para prevenir posibles fallos de eléctricos
- El cableado esta desprotegido y a la vista por el suelo
- Los equipos IT no cuentan con un cronograma de mantenimiento programado.
- Los equipos no cuentan con el hardware necesario para realizar actividades
- Los proveedores de servicios cuentan con disponibilidad variable para atender los servicios.
- El servidor cuenta con aplicaciones y programas free.
- 7 personas aceden a la red de internet
- 7 dispositivos se conectan a la red de internet
- La empresa cuenta con 5 Mb de internet
- El nivel de seguridad que presta el proveedor de internet es básico
- No cuentan con el conocimiento necesario para no caer en estafas por medio de mensajes por correo electrónico
- Existen dos niveles de privilegios en el sistema, los administradores y los usuarios
- La contraseña que se tiene contiene letras y números intercalados
- La oficina cuenta con el escritorio despejado y limpio
- No se realizan capacitaciones a sus usuarios y clientes sobre seguridad.
- Aparte de sistema utilizan otras aplicaciones que utilizan ancho de banda
- Disponen de un software de asistencia remota
- El sistema se desconecta por inactividades
- El sistema es lento, dado que algunas aplicaciones son virtualizadas

8.6 EVALUACIÓN ANÁLISIS Y GESTIÓN DE LOS RIESGOS

- La empresa no cuenta con políticas de seguridad

  No hay documentación de los diferentes procesos propios ni de manuales de uso de la plataforma.

  El riesgo es que no se cuenta con la suficiente información de las operaciones Internas, las políticas de seguridad permiten que se tenga en cuenta cada uno de los aspectos a tener en cuenta para evitar posibles fallos de seguridad de la información

- El cableado y los computadores no están protegidos contra eventualidades climáticas, el cableado y los computadores están muy cerca del suelo

  El cableado de red de Internet está muy mal distribuido esto puede ocasionar accidentes y caídas de red

  Se recomienda que se redistribuya el cableado de una manera que no genere inconvenientes

- Los equipos IT no están protegidos ante eventualidades

  Ningún equipo IT se encuentra asegurado, no existen pólizas.

- Todos los equipos electrónicos cuentan con ups para prevenir posibles fallos de eléctricos

  Los equipos de cómputo y equipos de red son conectados a ups que ayudan a proteger ante alguna caída de energía eléctrica o desbalances de voltaje

- Los equipos IT no cuentan con cronogramas de mantenimiento programado

  No se encuentran bitácoras e información de despliegues ni cronogramas de mantenimiento a los equipos y procesos.

- Los equipos IT no cuentan con el hardware necesario para realizar actividades

  Todos los equipos cuentan con limitaciones mínimas de funcionamiento, esto provoca que el sistema y los programas funcionen con lentitud.

- El servidor cuenta con aplicaciones y programadas free.

  El servidor cuenta con sistema operativo Linux, se maneja open suse dadas sus características de robustez.

- 7 personas aceden a la red de internet

Si, se conecta mucha gente a la red de Internet va a provocar lentitud en la red volviendo lento los procesos de la empresa.

- 7 dispositivos se conectan a la red de internet

  Los dispositivos móviles que se conectan a las redes Wi-Fi consumen mucho ancho de banda y esto ocasiona lentitud.

- La empresa cuenta con 5 Mb de internet

  Cinco megas de capacidad de descarga es muy poco para el número de equipos que hay.

  Se recomienda instalar por lo menos 10mb para que alcancé a realizar las actividades necesarias con más fluidez

- No cuentan con el conocimiento necesario para no caer en estafas por medio de mensajes por correo electrónico

  Los empleados no tienen los conocimientos para evitar caer en trampas por medio de los mensajes que llegan por correo.

- La oficina cuenta con el escritorio despejado y limpio

  La oficina no cuenta con un orden que proporcione una facilidad de movimiento.

  Los gabinetes y mesas escritorios deben estar organizados y ubicados de una forma que no dificulte el movimiento.

- No se realizan capacitaciones de seguridad a los empleado y clientes

  Al no realizar capacitaciones no se puede garantizar la calidad de los servicios.

  Un personal sin capacitar no estará preparado para las nuevas situaciones que se presenten a nivel de seguridad.

8.7 MAPA DE CALOR, PROBABILIDAD / CONSECUENCIAS

A continuación, se relaciona la escala de nivel de impacto

Tabla 24 Escala nivel impacto

	Bajo			Medio			Alto		
Nivel de Impacto	1	2	3	4	5	6	7	8	9

Fuente: El autor

A continuación, se relaciona la medición del rango de magnitud de daño

Tabla 25 Rango Magnitud daño

	Baja	Mediana	Alta
Magnitud del daño	1	2	3

Fuente: El autor

A continuación, se relaciona la probabilidad de amenaza

Tabla 26 Probabilidad Amenaza

	Baja	Mediana	Alta
Probabilidad amenaza	1	2	3

Fuente: El autor

A continuación, se evidencia las amenazas y probabilidad de la empresa algorítmicos

Tabla 27 Amenazas - probabilidad Algoritmicos

ACTIVOS - MAGNITUD DEL DAÑO (BAJA = 1) (MEDIANA = 2) (ALTA = 3)	AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA = 1) (MEDIANA = 2) (ALTA = 3)												
	Matriz De Riesgo Algoritmicos			DATOS		Hardware			Servicios				
				Manejo inadecuado de datos críticos	Transmisión no cifrada de datos críticos	Infección de sistemas a través de unidades portables	Falta de mantenimiento físico	Perdida de datos por error de hardware	Falta de actualización de software	Falla de software - corrupción	Virus	Fuga Informacion
				2	2	2	1	1	1	1	3	3
	Datos Digitales	Personales	1	2	2	2	1	1	1	1	3	3
		Legales	1	2	2	2	1	1	1	1	3	3
		Bases de datos	3	6	6	6	3	3	3	3	9	9
		Copias de seguridad	3	6	6	6	3	3	3	3	9	9
	Hardware IT	Dispositivos de almacenamiento	2	4	4	4	2	2	2	2	6	6
		Modem	2	4	4	4	2	2	2	2	6	6
		Servidor	3	6	6	6	3	3	3	3	9	9
		Equipo Escritorio	2	4	4	4	2	2	2	2	6	6
		Portatil	2	4	4	4	2	2	2	2	6	6
	Servicios IT	Webmin	2	4	4	4	2	2	2	2	6	6
		Servicio Proxy	1	2	2	2	1	1	1	1	3	3
		Servicio Backup	3	6	6	6	3	3	3	3	9	9
		Servicio Telnet	1	2	2	2	1	1	1	1	3	3
		Servicio Escritorio Remoto	1	2	2	2	1	1	1	1	3	3
		Servicio Web	2	4	4	4	2	2	2	2	6	6
		Servicio FTP	2	4	4	4	2	2	2	2	6	6

Fuente: El autor

9. DISEÑO DEL SGSI EN LA EMPRESA ALGORITMICOS M&C

Según la evaluación de las amenazas y los riesgos el diseño del SGSI se hará en cuatro pasos de la siguiente manera para el cumplimiento de la prevención del total de los riesgos y mejoramiento de las condiciones de trabajo

EL DISEÑO SE REALIZARÁ EN 4 PASOS: ADECUACIONES, CAPACITACIÓN, MANTENIMIENTO Y PROTECCION DE LA INFORMACION.

1) Adecuaciones Del Local Con El Fin De Mejorar Las Condiciones De Trabajo Y Evitar Amenazas Por La Mala Infraestructura

Las Adecuaciones del local con el fin de mejorar las condiciones de trabajo y evitar amenazas por la mala infraestructura fueron informadas al dueño de la empresa para que realizase las respectivas mejoras,

Las mejoras propuestas fueron las siguientes:

- Proteger el total del cableado de red eléctrica y de internet en canaletas por separado por lo menos a una altura de 50 centímetros en la pared.
- Ordenar las mesas de los ordenadores de una manera que se mejore la movilidad del personal.
- Las mesas tengan separaciones y tablas que impidan la visualización de las acciones realizadas en los monitores esto con el fin de proteger la confidencialidad de información sensible.
- La oficina, escritorios, sitios de trabajo siempre debe estar limpios y despejados

2) CAPACITACIÓN

Capacitación a todo el personal en donde incluiremos temas referentes a la seguridad de la información y seguridad informática, para evitar pérdidas de información y evitar que caigan en trampas de hackers que quieran acceder a la red.

La charla incluirá los siguientes temas:

- La recomendación para que lean los manuales y políticas de seguridad de la información para que tengan más claro cómo protegerse.
- Hablar sobre los diferentes permisos y privilegios que tiene cada empleado dependiendo de su función ya que no se están respetando las funciones.
- Se les recomendara que no conecten tantos dispositivos a la red de internet debido a que la red no tiene muchos megas de navegación y eso saturaría el ancho de banda haciendo que las tareas propias de la empresa se vean afectadas por la lentitud del sistema
- Lo más recomendable seria contratar un servicio de internet que brinde una mayor velocidad de carga y descarga de por lo menos 10 mega bytes.
- La seguridad y protección de la información en lo más importante en una organización por esa razón se expondrá extensamente una serie de diapositivas que explicaran de manera detallada las maneras de cómo proteger la información a la vez que se estará hablando de las diferentes técnicas y aplicaciones utilizadas por los hackers para realizar ataques esto con el fin que estén prevenidos ante este tipo de eventualidades.

3) Mantenimiento

Mantenimiento a todos los equipos tecnológicos, procesos y aplicaciones. Para evitar la lentitud por el exceso de aplicaciones y daños en los equipos, también para que el software importante corra con más fluidez

El mantenimiento incluirá las siguientes actividades.

- Formato de control del Mantenimiento detallado, donde se especifique fecha hora, responsable y procesos de cada mantenimiento.
- Ejecución de copias de seguridad

4) Protección De La Información

Para la protección de la información se realizarán las siguientes medidas de seguridad

- Procedimiento de autenticación de usuario y control de acceso, tanto para la visualización como para el tratamiento de los datos
- Instalar, utilizar y mantener actualizados cada actualización del sistema operativo.
- Garantizar la seguridad de la conexión a Internet.

- Instalar, utilizar y mantener actualizados cortafuegos de software en todos los ordenadores utilizados en la empresa.
- Revisar y mantener al día los parches de seguridad y actualizaciones de los sistemas operativos y aplicaciones. Todos los proveedores de sistemas operativos ofrecen parches y actualizaciones a sus productos para corregir los problemas de seguridad y para mejorar la funcionalidad.
- Controlar el acceso físico a los equipos y componentes de la red. No se debe permitir que las personas no autorizadas tengan acceso físico a los equipos, y se deben extremar las precauciones con el personal contratista.
- Asegurar el punto de acceso inalámbrico a las redes de trabajo, utilizando contraseñas fuertes y robustas.
- Configurar cuentas de usuario individuales para cada empleado en los equipos y en las aplicaciones de la empresa, con sus respectivas contraseñas
- Limitar el acceso de los empleados a los datos y la información específica que necesitan para hacer su trabajo.

10. CONCLUSIONES

Tras haber concluido el desarrollo de proyecto al final de la Especializacion, es el momento de efectuar el análisis y balance del resultado final obtenido, para poder obtener conclusiones, comprendidas de distintos aspectos, como lo técnico y profesional en el desarrollo de sistema de gestión de seguridad de la información.

Con este proyecto se ha conseguido ampliar conocimientos que se tenían sobre las asignaturas, Fundamentos de seguridad informática, Riesgo y Control Informático, Modelos y Estándares de seguridad informática, desde otro punto de vista, la realización de este sistema de gestión de la seguridad ha servido para descubrir un gran interés por la seguridad de la información.

Mediante el análisis llevado a cabo de la empresa Algoritmos M & C, en relación a controles de seguridad hacia el desarrollo de sus procesos y servicios, se diseña y socializa un sistema de gestión de la seguridad de la información, el cual es necesario para la entidad, no solo estará cumplimiento con los más altos de estándares de seguridad a la fecha, sino también mejorará cada uno de sus procesos y controles internos debido a la identificación y análisis de las vulnerabilidades.

No obstante, es muy importante desde la gerencia establecer la implementación del SGSI y su cumplimento en poder generar una cultura de seguridad en todas las áreas y miembros que la constituyen, porque los cambios no siempre son aceptados con facilidad, esto con el fin de que el SGSI genere un alto nivel de seguridad en sus procesos.

De acuerdo a la investigación desarrollada se deduce que por más que se realice la implementación del SGSI no se puede garantizar el 100% de la seguridad, dado que el propósito del SGSI es gestionar los riesgos de la información, es decir que sean conocidos, gestionados y minimizados por la organización.

11. RECOMENDACIONES

- ✓ Impulsar este proyecto en su implementación aplicando el diseño del sistema de gestión de la seguridad de la información propuesto y planteado, con el fin de mitigar y establecer los controles planteados así mismo las políticas de seguridad establecidas y planteadas en el proyecto.

- ✓ Para reestructurar el diseño del sistema de Gestion de seguridad de la información hay que tener en cuenta el conocimiento básico sobre el tema, por lo que se recomienda la orientación de un profesional en seguridad informática.

12. BIBLIOGRAFÍA

1. KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 251.

2. KOSUTIC, D. Business continuity plan: How to structure it according to ISO 22301. En Línea. Septiembre de 2014. Disponible en ISO 27001 & ISO 22301: (http://blog.iso27001standard.com/2012/09/24/business-continuity-plan-how-tostructure-it-according-to-iso-22301/)

3. KOSUTIC, D. ¿Cómo obtener la certificación ISO 27001? En Línea. 2 de Abril de 2010. Disponible en ISO 27001 & ISO 22301: (http://blog.iso27001standard.com/es/tag/sgsi/)

4. KOSUTIC, D. Lista de documentación obligatoria requerida por ISO/IEC 27001. En Línea. Septiembre de 2014. Disponible en ISO 27001 Academy: (http://www.iso27001standard.com/es/descargas-gratuitas/scrollTo-11725)

5. MAGERIT– versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

6. MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Universidad Javeriana. Disponible en: http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20K%20MG-05%20Manual%20del%20Sistema%20de%20Gestion%20de%20Seguridad%20de%20la%20Informacion.pdf

7. ODESHINA, N. ISO/IEC 27001:2005 Implementation and Certification—Doing It Again and Again. En Línea. Diciembre de 2013. Disponible en ISACA Journal:(http://www.isaca.org/Journal/Past-Issues/2013/Volume-2/Pages/ISOIEC-27001- 2005-Implementation-and-Certification-Doing-It-Again-and-Again.aspx)

8. NTC-ISO-IEC 27001:2013, Pág. 11-12, http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/N orma.%20NTC-ISO-IEC%2027001.pdf

9. RYAN, M., MARTIN, J. L. Information Security Risk Assessment Toolkit: Practical Assessment Through Data Collection and Data Analysis. Syngress. 2013. p. 13-18.

10. POVEDA, José. Análisis y valoración de los riesgos-Metodologías. Artículo. Bogotá D.C.: Universidad Católica de Colombia. Programa de Ingeniería de Sistema, 2013. 63 p. En: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

11. PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo. (25, agosto, 2015). En: http://www.magazcitum.com.mx/?p=2193. 231

12. STEWART, J. M., TITTEL, E., CHAPPLE, M. CISSP: Certified Information Systems Security Professional Guide (Quinta ed.). Indianapolis, Indiana, Estados Unidos de América: Wiley Publishing. 2011. p. 238.

13. ¿Seguridad informática o seguridad de la información? (25, septiembre, 2015) En: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-oseguridad-de-la.html

14. VITA. Information Technology Risk Management Guideline. En Línea. Noviembre de 2014. Disponible en Virginia Information Technology Agency: (https://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Word_versions/Risk_Ass essment_Instructions.doc)

15. WORDPRESS. Gestión de Riesgos en la Seguridad. Informática. (02, marzo, 2015) En: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

16. ZAWADA, B., & MARBAIS, G. Implementing ISO 2230: The Business Continuity Management System Standard. En Línea.Marzo de 2015. Disponible en Avalution Consulting: (http://www.avalution.com/system/cms/files/files/000/000/072/original/Implementing_ISO_22301.pdf)

Fecha de Realización:	28/07/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Trabajo Aplicado
Título:	DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ALGORÍTMICOS M&C
Autor(es):	Mesa Mendivelso Luis Manuel
Palabras Claves:	Gestion, Seguridad, Riesgo, Diseño.
Descripción:	Actualmente, en un mundo globalizado, donde prima el crecimiento tecnológico, las entidades buscando ser más competitivas, fortalecen metodologías operativas, para lograr procesos más eficientes y flujo de datos efectivos, por ello, la información generada en el transcurso de sus actividades, paso a ser un Activo de gran valor, en consecuencia, es fundamental adoptar medidas para asegurarlo y protegerlo, mitigando riesgos a nivel estructural e individual dentro de la organización, puesto que, sin importar su tamaño, es igual de vulnerable. Para salvaguardar de manera eficaz dicho Activo, la Organización Internacional de Normalización (ISO), asegura que toda empresa puede obtener Certificación ISO 27001, una norma diseñada para gestionar de forma segura la información, la cual se caracteriza por ser aplicable en cualquier tipo de empresa. En ésta síntesis, mediante un desarrollo contextual, se da a conocer el diseño de un Sistema de Gestión de Seguridad de la Información, para la empresa Algoritmos M & C, basado en la Norma Internacional ISO 27001, mediante recolección de información, inventario de activos, análisis de riesgos, identificaciones de vulnerabilidades y amenazas, para establecer controles y políticas de seguridad, las cuales brindan recomendaciones y acciones, permitiendo mostrar un panorama general en cuanto a su seguridad informática limitado a procesos generales de la empresa que estén documentados.

Fuentes bibliográficas destacadas:

[1] AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN, Tarazona, H Cesar, Universidad Externado {En línea}. revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

[2] ISO 27001:2013 – SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN En línea. Noviembre 2017 Disponible en: http://www.sgs.co/es-es/health-safety/quality-health-safety-and-environment/risk-assessment-and-management/security-management/iso-27001-2013-information-security-management-systems

[3] KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 251

[4] KOSUTIC, D. Business continuity plan: How to structure it according to ISO 22301. En Línea. Septiembre de 2014. Disponible en ISO 27001 & ISO 22301: http://blog.iso27001standard.com/2012/09/24/business-continuity-plan-how-tostructure-it-according-to-iso-22301

[5] RYAN, M., MARTIN, J. L. Information Security Risk Assessment Toolkit: Practical Assessment Through Data Collection and Data Analysis. Syngress. 2013. p. 13-18.

[6] PRANDINI, Patricia y PALLERO, Marcela. Vulnerabilidades, amenazas y riesgo. (25, agosto, 2015). En: http://www.magazcitum.com.mx/?p=2

[7] ¿Seguridad informática o seguridad de la información? (25, septiembre, 2015) En: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-oseguridad-de-la.html

Contenido del documento:	OBJETIVO GENERAL Diseñar un sistema de gestión de Seguridad de la Información, en la empresa ALGORITMICOS M&C, bajo los lineamientos del Estándar Internacional ISO 27001 para seguridad de la información. OBJETIVOS ESPECÍFICOS

	• Ejecutar una revisión del estado actual de la seguridad de la Información en la empresa Algorítmicos M&C. • Realizar análisis y evaluación de las vulnerabilidades, mediante la matriz de riesgos. • Gestionar los riesgos encontrados mediante la aplicación de controles, tomando como referencia la norma ISO 27001 RESUMEN Este artículo se presentará proponer y diseñar un sistema de gestión para la seguridad de la información, cuya función sea garantizar que los riesgos expuestos anteriormente sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios en el flujo o manejo diario de la información.
Marco Metodológico:	Para éste proyecto, se implementa un enfoque metodología - analítico, ya que, permite descomponer el todo del problema en partes o elementos más pequeños, con el fin de conocer la causas de su origen, puesto que, se necesita conocer la naturaleza del problema para poderlo entender , junto con la metodología inductiva, la cual complemente en forma adecuada a la práctica, debido a sus componentes esenciales que conllevan cuatro pasos: observación, clasificación, derivación inductiva y contrastación; con la finalidad de brindar hipótesis aplicables a la obtención de una solución del problema. Los pasos a seguir serán tomados de la siguiente manera: Recolección de la información: Se recopiladora la información la información de la empresa mediante inventario de activos, encuestas y cuestionarios personalizados según perfiles de los colaboradores.

	Muestras: Como muestra al ser una pequeña empresa inferior a 10 colaboradores, tomaremos el 100% de los empleados. Procesamiento de la información: La información recolectada se analizará y clasificará para identificar amenazas, vulnerabilidad y riesgos con el objetivo de elaborar controles y una política de seguridad.
Conceptos adquiridos :	Con este proyecto se ha conseguido ampliar conocimientos que se tenían sobre las asignaturas, Fundamentos de seguridad informática, Riesgo y Control Informático, Modelos y Estándares de seguridad informática, desde otro punto de vista, la realización de este sistema de gestión de la seguridad ha servido para descubrir un gran interés por la seguridad de la información. Mediante el análisis llevado a cabo de la empresa Algoritmos M & C, en relación a controles de seguridad hacia el desarrollo de sus procesos y servicios, se diseña y socializa un sistema de gestión de la seguridad de la información, el cual es necesario para la entidad, no solo estará cumplimiento con los más altos de estándares de seguridad a la fecha, sino también mejorará cada uno de sus procesos y controles internos debido a la identificación y análisis de las vulnerabilidades
Conclusiones:	Tras haber concluido el desarrollo de proyecto al final de la Especializacion, es el momento de efectuar el análisis y balance del resultado final obtenido, para poder obtener conclusiones, comprendidas de distintos aspectos, como lo técnico y profesional en el desarrollo de sistema de gestión de seguridad de la información. No obstante, es muy importante desde la gerencia establecer la implementación del SGSI y su cumplimento en poder generar una cultura de seguridad en todas las áreas y miembros que la constituyen, porque los cambios no siempre son aceptados con facilidad, esto con el fin de que el SGSI genere un alto nivel de seguridad en sus procesos.

	De acuerdo a la investigación desarrollada se deduce que por más que se realice la implementación del SGSI no se puede garantizar el 100% de la seguridad, dado que el propósito del SGSI es gestionar los riesgos de la información, es decir que sean conocidos, gestionados y minimizados por la organización