DISEÑO E IMPLEMENTACION DE UNA POLÍTICA DE SEGURIDAD DE INFORMACIÓN, EN EL GRUPO DE TRABAJO CUENTAS POR PAGAR DEL MINISTERIO DE TRANSPORTE.

MARIA ELENA MARIN OSPINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO E IMPLEMENTACION DE UNA POLÍTICA DE SEGURIDAD DE INFORMACIÓN, EN EL GRUPO DE TRABAJO CUENTAS POR PAGAR DEL MINISTERIO DE TRANSPORTE.

MARIA ELENA MARIN OSPINA

Proyecto Aplicado

Ingeniero de Sistemas
Hernando Jose Peña Hidalgo
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
NOVIEMBRE 2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá 22, noviembre, 2017

CONTENIDO

pág.

INTRODUCCIÓN 10

1. TITULO 11

2. DEFINICIÓN DEL PROBLEMA 12

2.1 ANTECEDENTES 12

2.2 FORMULACION 13

2.3 DESCRIPCIÓN 14

3. JUSTIFICACIÓN 15

4. OBJETIVOS 16

4.1 OBJETIVO GENERAL 16

4.2 OBJETIVOS ESPECIFICOS 16

5. MARCO REFERENCIAL 17

5.1 ANTECEDENTES 17

5.2 MARCO CONTEXTUAL 18

5.3 MARCO TEORICO 20

5.4 MARCO CONCEPTUAL 26

5.5 MARCO LEGAL 27

6. ALCANCE Y DELIMITACIÓN DEL PROYECTO 31

6.1 ALCANCE 31

6.2 DELIMITACIÓN 31

7. METODOLOGÍA 33

8. DESARROLLO DEL PROYECTO.....34

8.1 CARACTERIZACIÓN RECURSOS DE INFORMACIÓN ADMINISTRADOS POR EL GRUPO DE CUENTAS POR PAGAR 34

8.1.1 Base de datos relación de pagos.....34

8.1.2 Base de datos administración documental.....38

8.1.3 Base de datos servicios públicos 40

8.1.4 Base de datos control cuentas por pagar.....43

8.2 RECOLECCION DE INFORMACIÓN SOBRE SEGURIDAD INFORMATICA EN EL GRUPO DE CUENTAS POR PAGAR.....45

9. ANALISIS SITUACION ACTUAL DEL MANEJO DE LA INFORMACIÓN DIGITAL EN EL GRUPO CENTRAL DE CUENTAS POR PAGAR.....62

9.1 SITUACIÓN ACTUAL 62

9.2 ANALISIS DE LA SITUACION ACTUAL DEL GRUPO CUENTAS POR PAGAR EN SEGURIDAD INFORMÁTICA.....63

9.2.1 Análisis del contenido de política de seguridad del Mintic 63

9.2.2 Análisis del contenido de política de seguridad del ministerio de transporte 65

9.2.3 Análisis del Contenido del Documento de Normas ISO.....69

9.2.4 Análisis del contenido del documento CONPES 3854.....71

9.3 ANALISIS DE CRITERIOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL, AL ESTUDIO DE CASO DEL GRUPO DE CUENTAS POR PAGAR.....72

10. DISEÑO ESTRUCTURA DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA PARA EL GRUPO CUENTAS POR PAGAR 75

11. DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL GRUPO CUENTAS POR PAGAR. 77

CONCLUSIONES 91

BIBLIOGRAFIA.....92

ANEXOS.....96

LISTA DE TABLAS

pág.

Tabla 1. Matriz de metodología.....33

Tabla 2. Análisis encuesta 48

Tabla 3. Políticas para la seguridad de la información.....79

Tabla 4. Políticas de uso de computador personal y del software instalado.....80

Tabla 5. Políticas de acceso 82

Tabla 6. Políticas de no repudio.....83

Tabla 7. Políticas de privacidad y confidencialidad de la información.....84

Tabla 8. Políticas de integridad de la información.....85

LISTA DE ILUSTRACIONES

pág.

Ilustración 1. Organigrama Ministerio de Transporte 19

Ilustración 2. Análisis grafico pregunta 1 51

Ilustración 3. Análisis grafico pregunta 2 52

Ilustración 4. Análisis grafico pregunta3 53

Ilustración 5. Análisis grafico pregunta 4 54

Ilustración 6. Análisis grafico pregunta 5 54

Ilustración 7. Análisis grafico pregunta 6 55

Ilustración 8. Análisis grafico pregunta 7 56

Ilustración 9. Análisis grafico pregunta 8 56

Ilustración 10. Análisis grafico pregunta 9 57

Ilustración 11. Análisis grafico pregunta 10 57

Ilustración 12. Análisis grafico pregunta 11 58

Ilustración 13. Análisis grafico pregunta 12 59

Ilustración 14. Análisis grafico pregunta 13 59

Ilustración 15. Análisis grafico pregunta 14 60

Ilustración 16. Análisis grafico pregunta 15 61

LISTA DE ANEXOS

pág.

Anexo A Formato RAE.....96

Anexo B Instrumento evaluación MSPI…….98

INTRODUCCIÓN

El Ministerio de Transporte es una entidad del Estado, encargada de formular las políticas para el transporte a nivel nacional en los modos fluvial, férreo, aéreo y terrestre.

En el año 2008 se creó una política de seguridad informática de manera general, pero a la fecha no se le ha realizado ninguna modificación o actualización y en cambio sí han surgido cambios en la estructura orgánica del ministerio, avances en tecnologías informáticas, tanto en hardware como software.

En el grupo de Central de Cuentas por Pagar del Ministerio de Transporte, se realizan todos los pagos a proveedores y contratistas a nivel nacional; usando información digital en bases de datos que controlan todas las cuentas por pagar, administración documental, relación de pagos y servicios públicos. Siendo información digital de gran importancia, está muy expuesta a manipulación sin la seguridad necesaria.

Con el desarrollo del presente proyecto se busca diseñar e implementar una política de seguridad informática, dirigida a la información digital que se maneja en el Grupo de Cuentas por Pagar; hacer seguimiento y actualización a esta política y la debida socialización; no solo a nivel de grupo, sino a nivel Subdirección Administrativa y Financiera; pues en cada grupo se maneja información digital diferente; pero en las que se puede implementar esta política de seguridad informática-

1. TITULO

DISEÑO E IMPLEMENTACION DE UNA POLÍTICA DE SEGURIDAD DE INFORMACIÓN, EN EL GRUPO DE TRABAJO CUENTAS POR PAGAR DEL MINISTERIO DE TRANSPORTE.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES

El Ministerio de Transporte actualmente está organizado por el despacho del Ministro, el despacho del Viceministro, Secretaria General con oficinas de control interno, planeación, informática, jurídica y prensa, dos subdirecciones la administrativa y financiera y la de talento humano; cada una de estas subdirecciones está dividida en grupos de trabajo por tema. Cada uno de estos grupos maneja diversas informaciones digitales con requerimientos de seguridad diversos, de mayor o menor rigurosidad. Esta Entidad tiene una política de seguridad informática que presenta lineamientos generales para todos los grupos que estructuran el Ministerio, fue publicada en el año 2008 y a través de estos 9 años no se le ha realizado revisión ni actualización, además no ha tenido la socialización necesaria para su apropiación.

Específicamente el Grupo de Cuentas por Pagar tiene altos requerimientos de seguridad que actualmente no son tenidos en cuenta y que pueden ser un riesgo potencial para la manipulación, modificación y pérdida de información digital.

Incidentes de seguridad presentados en el Grupo de Cuentas por Pagar:

- Perdida de información ya registrada, por la manipulación de bases de datos por muchos funcionarios sin la debida encriptación y sin el debido conocimiento; produciendo errores de doble registro, registros incompletos, eliminación de información.

- Perdida de tiempos y registros, por la mala planeación del uso de la base de datos de control de cuentas por pagar; al ser manipulada, por varias personas a la vez, cuando solo a una le deja grabar.

- Reconstrucción de toda una base de datos, por la no existencia de control en las copias de seguridad de ninguna de las bases de datos; y al estar tan expuestas; fácilmente por error o a propósito puede ser borrada la información.

- Errores al emitir informes, estadísticas y conciliaciones, con la base de datos de servicios públicos por tener muchos campos de registros que no se usan y que no se han actualizado con las necesidades reales.

- Archivos físicos dobles de los pagos de servicios públicos.

- A la base de datos de relación de pagos, ya no se le pueden ingresar más datos, por falta de espacio en el aplicativo.

- Anulación de radicados por mal uso como: mal ingreso de remitentes, de destinatarios, un oficio lo han enviado con plantilla de memorando y un memorando con plantilla y código de oficio, descontrolando el sistema; se han descargado documentos que aún no han tenido el tramite completo; aunque la anulación y ciertos privilegios en el aplicativo solo los tiene el Coordinador del grupo; por tener un acceso muy vulnerable; fácilmente se puede transferir los permisos para que otro funcionario del grupo haga uso de ellos.

Se evidencia, por tanto, que hace falta una política de seguridad informática, actualizada y que responda a necesidades puntuales de rigurosidad de seguridad en cada grupo de trabajo; en este caso al Grupo de Central de Cuentas por Pagar.

Es fundamental que dicha política de seguridad establezca principios de seguimiento, evaluación, revisión y actualización, con el fin de asegurar su utilidad y gestión.

2.1 FORMULACION

¿Cómo diseñar e implementar política de seguridad de información para el grupo de trabajo de cuentas por pagar del Ministerio de Transporte?

Se toma como referencia para el diseño e implementación de políticas de seguridad, el análisis a la situación actual de la información en el Grupo Central de Cuentas por Pagar, Políticas de Seguridad del MINTIC, Políticas de Seguridad de Ministerio de Transporte, análisis de contenidos de la norma ISO y del documento CONPES 3854.

2.2 DESCRIPCIÓN

Viendo todas las deficiencias de seguridad de la información en el Grupo de Cuentas por Pagar, se hace necesario diseñar e implementar una política de seguridad de información en el grupo de cuentas por pagar; para planear, controlar, seguir y mantener los procesos que se desarrollan en el grupo de una forma segura.

Si no se implementa la política de seguridad, se estará expuesto a pérdida o mal uso de la información y por ende a procesos inseguros y con muchas falencias.

El diseño e implementación de la política de seguridad para el Grupo de Cuentas por Pagar, se debe realizar por los niveles de inseguridad vistos y porque la actual política de seguridad que tiene el Ministerio está dada de forma general y no está actualizada.

3. JUSTIFICACIÓN

Al tener un adecuado manejo de la seguridad y blindaje de la información digital administrada por el grupo de cuentas por pagar, las relaciones de pagos, la administración documental y los pagos de servicios públicos; redundara en información concreta y veraz de todos los pagos realizados en el Ministerio de Transporte no solo en planta central sino en las Direcciones Territoriales e Inspecciones Fluviales.

La finalidad con este proyecto es implementar un documento de política de seguridad de la información digital en el grupo de trabajo Cuentas por Pagar del Ministerio de Transporte.

Una vez diseñadas las políticas de seguridad, deberán ser aplicadas por medio de la Coordinación del Grupo de Cuentas por Pagar, en cada una de las aplicaciones digitales del Grupo; beneficiándose no solo los funcionarios del Grupo sino cada una de las áreas a nivel central y nacional.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar e implementar política de seguridad en la información que permita prevenir los riesgos que se presentan en la manipulación y manejo de información digital específicamente en el grupo de cuentas por pagar del Ministerio de Transporte.

4.2 OBJETIVOS ESPECIFICOS

- Caracterizar los recursos de información administrados por el Grupo Cuentas por Pagar: “relación de pagos”, “administración documental” “servicios públicos” y “cuentas por pagar”.

- Analizar situación actual del manejo de la información digital en el Grupo de Cuentas por Pagar e identificar vulnerabilidades y amenazas.

- Aplicar el análisis de criterios de la política de seguridad de la información digital, al estudio de caso del Grupo de Cuentas por Pagar.

- Diseñar documento digital con la política de seguridad de información para el grupo de Cuentas por Pagar.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

La presente investigación plantea unos antecedentes que son base para el desarrollo y planteamiento del proyecto aplicado, entre estos antecedentes se encuentra, por un lado, el modelo de seguridad y privacidad de la información del Mintic, la Política de Seguridad Informática del Ministerio de Transporte, tesis y monografías que nos proporcionaran información general sobre seguridad informática.

Inicialmente se aborda el Modelo de Seguridad y Privacidad de la Información (MSPI), documento realizado por el Mintic, en el cual se da a conocer una serie de guías paso a paso, para desarrollar modelos de seguridad en cuanto a políticas, procedimientos, gestión, controles, auditorias entre otros. (Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia (Mintic), s.f.)

El Mintic nos proporciona un documento creado en el año 2016, que servirá de guía para elaboración e implementación de la política general de seguridad y privacidad de la información. (Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic), 2016)

Por otro lado, se tiene la Política de Seguridad Informática del Ministerio de Transporte publicada en el año 2008 por el grupo de informática de esta entidad que fue el encargado de la elaboración de la política, este documento tiene por objeto definir las normas y procedimientos que los funcionarios del Ministerio de Transporte deben poner en práctica con el fin de asegurar el uso adecuado de los recursos informáticos.

Luis Daniel Álvarez Basaldúa, presenta su tesis sobre seguridad en informática, que nos da una guía sobre la planeación, uso, responsabilidades en la red; políticas de seguridad; auditorias de sistemas; seguridad en centros de cómputo y algo muy importante a tener en cuenta que son estándares internacionales en tecnología de información. (Alvarez Basaldúa, 2005).

Estudiantes de la Universidad de Bío-Bío de Chile, presentan un artículo sobre los modelos para seguridad de la información en TIC, realizando un énfasis a los controles de riesgos y así evitar o disminuir las fallas que se encuentran en los sistemas. (Burgos Salazar & Campos).

Alumnos de la Universidad Salesiana de Bolivia, presentan su monografía sobre seguridad en redes y teniendo en cuenta que dos de las bases de datos, en estudio están en la red, podemos tener en cuenta los objetivos y los modelos, de seguridad en redes que en esta monografía desarrollan. (Mayta Siles, y otros, 2011).

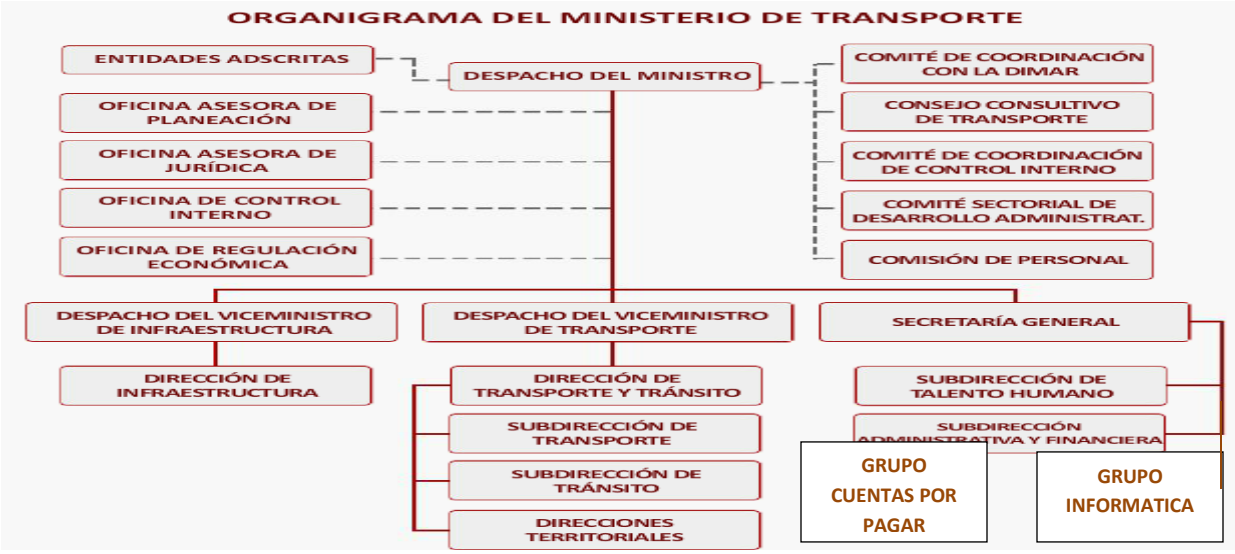
Para ubicarnos en cuanto a las políticas de seguridad en América Latina, se puede consultar el artículo de investigación de Egbert J. Sánchez Vanderkast, que nos presenta un estudio sobre la situación actual de las políticas de seguridad de la información en los países vecinos. (Sánchez Vanderkost).

Dentro de las bases de datos que son manejadas en el grupo Cuentas por Pagar del Ministerio de Transporte, se encuentran cuatro que son manipuladas a diario por cada uno de los funcionarios del grupo, y que además son fundamentales para llevar a cabo de forma efectiva la labor desempeñada dentro de la institución.

5.2 MARCO CONTEXTUAL

El Ministerio de Transporte es una entidad del orden nacional que se encarga de garantizar el desarrollo y mejoramiento del transporte en Colombia, básicamente el objetivo del Ministerio de Transporte es legislar las norma sobre transporte en todas sus modalidades (terrestre, aéreo, fluvial y férreo) y con estas normas velar por que el transporte en Colombia tenga una excelente infraestructura y calidad.

Ilustración 1. Organigrama Ministerio de Transporte



Fuente: www.mintransporte.gov.co

Para cumplir la misión y los objetivos, el Ministerio cuenta con dos tipos de áreas, las misionales y las de apoyo. Las áreas misionales son las encargadas de formular las políticas, regulaciones técnicas y económicas en transporte, transito e infraestructura.

Dentro de las áreas de apoyo para realizar estas políticas está el grupo de informática y la subdirección administrativa y financiera.

En la subdirección Administrativa y financiera, está el grupo de cuentas por pagar, que lleva el registro y control de todos los pagos que se hacen a nivel nacional a funcionarios, contratistas y proveedores, para este proceso, maneja los siguientes sistemas de información:

Relación de Pagos: Esta es una base de datos de Dbase, donde se registran los contratistas de tipo natural y jurídico; y se lleva el control de pagos y saldos de

cada uno de ellos. Sin esta relación de pagos no es posible liquidar los contratos que se tienen en el MT a nivel nacional.
Administración Documental: En este sistema de información se registran y digitalizan toda la correspondencia interna y externa del Ministerio de Transporte, se puede conocer el destino, y el histórico de un radicado, su importancia radica en que es la herramienta que utilizan tanto los funcionarios como agentes externos para verificar el estado de sus solicitudes.

Servicios Públicos: Este sistema de información mantiene el registro de los recibos de servicios públicos a nivel nacional, así como los pagos que se realizan, es manipulado por dos personas y presentan niveles de seguridad mínimos a pesar del manejo de dinero y la responsabilidad que esto significa en una entidad estatal.

Cuentas por Pagar: En este sistema de información se registra y controlan todos los pagos que realiza el Ministerio de Transporte a proveedores, contratistas, servicios públicos, funcionarios y ex funcionarios. Es la base de datos más vulnerable ya que está ligada a otras plataformas de la subdirección administrativa y financiera, además es manipulada por cuatro personas solo en el grupo de cuentas por pagar.

5.3 MARCO TEORICO

Se plantean a continuación las categorías principales que son el marco para el desarrollo de la investigación, entre estas se encuentran:

Sistema de Información: Un sistema de información son los elementos que se interrelacionan, y de los cuales se puede capturar, procesar, almacenar y transmitir los datos de la compañía, para generar información, confiable y a tiempo.

La información en toda organización debe ser:

- Importante
- Actualizada
- Rápida

- Económica
- De calidad
- Objetiva
- Completa
- Aplicable

Un sistema de información, debe estar compuesto por:

- Recursos físicos
- Recursos humanos
- Procedimientos

Seguridad de la información comprende todas las medidas, desarrollos y procedimientos encaminados a proteger de forma efectiva la información independiente del tipo, forma del almacenamiento o de transmisión. Las tres principales características de protección de la información son:

- Integridad
- Confidencialidad
- Disponibilidad

Seguridad informática: Teniendo claro lo que es seguridad de la información, la seguridad informática es una de sus ramas que en esencia busca proteger información que se encuentra enmarcada en una infraestructura informática o de telecomunicaciones**.** (Romero & Ramada, 2013) Existen algunos tipos de seguridad informática tales como:

- Seguridad física
- Seguridad lógica
- Seguridad activa
- Seguridad pasiva

Problemáticas: Se pueden presentar problemas cuando la información se vuelve vulnerable, es decir cuando hay debilidades en sus activos o agujeros de seguridad. Estos problemas se pueden asociar a fallos de implementación de las

aplicaciones, malas configuraciones de los sistemas operativos, descuido de la utilización de los sistemas entre otros. (ESCRIVA R.).

Principales amenazas de seguridad: de los sistemas de información y activos informáticos de las empresas (infraestructura tecnológica y de comunicaciones, hardware, software, persona, aplicaciones, acceso físico).

Las amenazas a la seguridad informática se pueden agrupar en:

- Factores humanos (accidentes, errores).
- Fallas en los sistemas de procesamiento de la información (fraudes basados en el uso de computadores, denegación de servicios (DOS), alteraciones de la información, divulgación de la información).
- Desastres naturales.
- Actos maliciosos o malintencionados (virus informáticos o código malicioso, uso no autorizado de sistemas informáticos, robo de información, suplantación de identidad, sabotaje, vandalismo, espionaje). (TARAZONA, s.f.)

Las amenazas más conocidas son:

- **Spyware**: código malicioso, programas espías para robar información, sin embargo, también podría usarse para controlar el uso de software pirata.

- **Troyanos**: virus y gusanos, son programas de código malicioso, permitiendo el acceso no autorizado de los atacantes y control de forma remota a los sistemas, bloquea y daña la información.

- **Phishing**: Obtiene de forma fraudulenta datos confidenciales de un usuario, aprovechando la confianza de los servicios tecnológicos y pocas medidas de seguridad.

- **Spam**: recibo de mensajes no solicitados, especialmente en correo electrónico, telefonía celular, mensajes de texto y faxes.

- **Botnets**: Redes de robots, maquias infectadas y controladas remotamente, estos robots envían mensajes masivos spam o código malicioso para atacar otros sistemas.

- **Trashing**: manejo de la basura, es una forma de ingeniería social, revisando en la basura para extraer información y poder definir un perfil de victima para robar identidad, o ingreso directo a la información. (TARAZONA, s.f.)

Principales amenazas de seguridad de la información de las personas.

- **Ingeniería social**: que es la conducta social destinada a conseguir información de las personas cercanas a un sistema por medio de habilidades sociales como engaños, tretas y artimañas. La persona víctima de esta ingeniería social compromete el sistema y revela información.

- **Adware**: es un programa malicioso que aprovecha descuido de los usuarios, se instala y descarga y muestre anuncios publicitarios en la pantalla de la víctima, aunque no daña el sistema si disminuye el rendimiento del equipo y de la navegación por la red. (Luzardo, 2010)

- **Ransomware**: La última modalidad delincuencial, con repercusiones a nivel mundial, que es la técnica que usan los hackers para bloquear dispositivos y exigir rescate a cambio de recuperar el acceso a la información robada. (Ransomware)

Tendencias: En el año 2016 las tendencias en cuanto a seguridad informática fueron:

- Vulnerabilidades y su gravedad
- Disminución de vulnerabilidades en Java
- Mejor protección en las empresas
- Globalización respecto a la seguridad de la información
- Aplicaciones nuevas muy vulnerables
- Altos niveles de troyanos
- Amenazas complejas

- Vulnerabilidad en plataformas. (Tendencias en Seguridad Informatica 2016, 2016).

Recursos Informáticos: Algunos de los recursos informáticos del Ministerio de Transporte que son objeto de análisis de esta política son:

- Sistemas de información y aplicación del negocio
- Software de oficina
- Sistema de correo electrónico
- Documentación en cualquier medio, óptico, magnético, papel.

Informática forense: Es una aplicación que permite conseguir pruebas digitales en un computador que está en investigación. Con estas aplicaciones se pueden encontrar y analizar, archivos ocultos, borrados, camuflados o dañados.

Los delitos informáticos y las respectivas investigaciones que se hagan para combatirlos, están amparados por la Ley 1273 de 2009. (Ing. Esp. Harold Emilio Cabrera Meza – UNAD, 2013).

Las aplicaciones de informática forense, nos dan la posibilidad de recoger todo tipo de evidencia en computadores móviles, fijos e inalámbricos; por ejemplo:
Bolsas Faraday; estas bolsas de un material especial, lo que hace es proteger y bloquear la señal del dispositivo que se encuentre en ella.

Bloqueadores de escritura: se bloquean los dispositivos y se evita que se hagan cambio o modificaciones.

Cadena de custodia: Resguarda la información, de tal manera que se conserven los originales de principio a fin de una investigación. (Rosa, 2014).

CSIRT: son equipos de personas con amplio conocimiento en informática, que podrán impartir controles y soluciones a daños ocasionados a la información de una organización; pueden hacer un seguimiento de principio a fin de un incidente, estableciendo causas, consecuencias y soluciones. (Mendoza, 2015)

Seguridad en redes: Hoy en día casi todos los equipos están conectados a una red LAN generalmente, cuando hay datos que salen y entran por interfaz de red, estas redes son vulnerables; hay protocolos seguros de red como HTTPS y SSH y protocolos inseguros como DHCP, DNS y HTTP.

Se deben tener en cuenta ciertas actividades para la seguridad en las redes como:

- Switch administrable: conmutador de red VLAN con autenticación en el puerto y estadísticas de tráfico.
- Control de acceso MAC (Medium Access Control), dirección de seis parejas de números hexadecimales, asignadas por el fabricante.
- Uso SSID identificador de red inalámbrica
- Se debe proteger el acceso físico, el acceso lógico con usuarios y contraseñas, controlar quien puede ingresar por medio de autenticaciones y realizar encriptación de transmisión. (BUENDIA, 2013)

Gestión de seguridad informática: con la implementación de un sistema de gestión de calidad en una organización, se tendrán las herramientas, para identificar vulnerabilidades, amenazas, riesgos y establecer los controles y por ende las soluciones pertinentes; a las tecnologías de información existentes.

Las organizaciones deben designar a las personas que se harán responsables del control de producción, desarrollo, mantenimiento, uso y seguridad de los activos.

Para un buen sistema de gestión de seguridad informática se deben definir alcances, limites, políticas, enfoques. Análisis y evaluación de riesgos, objetivos de control y controles, autorización de implementación y declaración de aplicabilidad. (Establecimiento y Gestión del SGSI, s.f.)

Políticas de Seguridad: Una política de seguridad, es un documento donde las directivas de una organización, se compromete a seguir y cumplir una serie de instrucciones y acciones con miras a obtener seguridad en la información.

Según la norma ISO 27001, el propósito de implementar una política de seguridad de la información, en una empresa es:

- Directivas conscientes de que tipo de seguridad de información quieren para su empresa.
- Documento fácil de entender y que sirva de guía, con objetivos claros de lo que se quiere lograr.
- Controlar el SGSI

Una política de seguridad de la información, debe:

- Adaptarse a las condiciones y situaciones precisas de la empresa.
- Objetivos claros de seguridad de la información
- Alta gerencia comprometida con cada requisito de la implementación de la política; para poder hacer seguimiento, control y mejoramiento continuo.
- Una vez realizada la política debe ser socializada en toda la organización, para asegurar su cumplimiento.
- La política debe actualizarse continuamente. (SGSI)

5.4 MARCO CONCEPTUAL

Activos Informáticos: Recursos del sistema de información, que tienen un valor y que deben ser protegidos.

Agujeros de seguridad: debilidades o vulnerabilidades en un sistema de información.

Amenazas: son todas las circunstancias que pueden atentar con un sistema informático establecido, estas amenazas pueden estar divididas entre las pasivas y las activas, dependiendo de si obtienen información o si realizan cambios sobre la misma. (Romero & Ramada, 2013).

Base de datos: agrupación de información interrelacionada, estructurada y organizada (Ministerio de Transporte, 2008) es fundamental que estas bases permitan acceso y manejo seguro de la información

Cuenta por Pagar: radicación de la cuenta por pagar, que llega al Grupo, esta radicación se realiza en el aplicativo SIIF.

Dbase: (Banda, 2002), es un software que crea, administra y almacena base de datos, en nuestro caso, se ingresan los datos de contratos, se va alimentando con los pagos mes a mes y se generan informes de los pagos realizados a los contratos.

Información digital: es información codificada que se encuentra procesada en un ordenador y que es fundamental para el funcionamiento de la entidad (Codina, 2001).

Obligación presupuestal: Registro realizado, en el aplicativo SIIF, para ingresar la ejecución de los gastos. (Cartilla Sistema SIIF Nación en el Ministerio de Defensa Nacional, s.f.)

Orfeo: es el aplicativo o software libre, licenciado por GNU/GPL de correspondencia que se maneja en el Ministerio de Transporte, administra todo documento ya sea escrito o digital, tanto interno como externo. (Orfeo, s.f.).

Sistema Integrado de Información Financiera de la Nación (SIIF): (Dirección Nacional de Planeación, s.f.), es una herramienta modular automatizada, que consolida la información financiera de todas las entidades de la nación.

Unidades ejecutoras de presupuesto: son divisiones o dependencias que ordenan gastos con cargo al presupuesto de la nación (Contaduria General de la Nación, s.f.), en los registros que se hacen en el Grupo de Cuentas por pagar se ingresa a unidades de gastos generales, Unidad de Movilidad Urbana Sostenible (UMUS) (UMUS, s.f.), sobretasa a la gasolina, Plan Vial Regional (PVR) (PVR, s.f.), Registro Único Nacional de Transito RUNT (RUNT, s.f.), Seguridad vial, Logística, Cooperación Internacional y Regalías o SGR (SGR, s.f.)

Vulnerabilidad: hace referencia a cualquier debilidad que implique una posibilidad de daño en el sistema informático.

5.5 MARCO LEGAL

Normas internacionales ISO: norma sobre políticas de seguridad comprende una serie de ítems que profundizan, así:

- Objeto y campo de aplicación
- Referencias normativas
- Términos y definiciones
- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño
- Mejora

Las normas internacionales ISO, nos da las herramientas para establecer los objetivos de control, siempre teniendo en cuenta los objetivos y las necesidades de las organizaciones y con el fin de que la información que se genere sea confiable, integra y disponible. (NTC-ISO/IEC 27001, 2013)

La normatividad aplicada a políticas de seguridad en Colombia es:

Norma internacional **ISO/IEC 27001- Sistema de Gestión de la Seguridad de la Información,** que especifica los requisitos para una adecuada gestión de la seguridad de la información (establecer, implantar, mantener y mejorar) según el PDCA (Planificar, Hacer, Verificar, Actuar). (Ministerio de Transporte, 2008)

Norma ISO 27002:2005/2013, sobre seguridad y controles de información. (ISO 27001 / 27002, s.f.).

Las ISO 27000 y 27001, son normas para aplicación a los sistemas de gestión, en cualquier tipo de empresa u organización, especifican los requisitos para la implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) documentado.

Como tienen en cuenta los riesgos y amenazas informáticas, estas normas explican cómo se debe diseñar un SGSI y como establecer los controles de seguridad, según necesidades. (Solarte, 2016).

La norma ISO 27001, en el anexo A5 – Politicas de Seguridad de la Información, presenta controles de la forma como se deben escribir y revisar, dichas politicas. (Advisera, s.f.)

El Ministerio de Tecnologías de la Información y Comunicaciones en Colombia (Mintic), tiene una serie de documentos, que sirven de ayuda para conocer sobre la seguridad de la información, los obstáculos, los ataques, la baja capacidad de respuesta, falta de conciencia, muchas plataformas y mala planeación y orden en las organizaciones; también brindan información de la forma en que se deben plantear los objetivos de las entidades como son : incrementar niveles de seguridad, implementar políticas de seguridad, implementar sistemas de gestión de seguridad informática y concientizar a funcionarios y usuarios de las entidades sobre la importancia y el impacto de la seguridad de la información. (Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia (Mintic), s.f.)

El Ministerio de Tecnologías de la información y Comunicaciones en Colombia (Mintic), nos suministra un instrumento de evaluación MSPI (Modelo de Seguridad y Privacidad de la Información), los formatos están establecidos y deberán ser diligenciados por cada entidad del estado. (Anexo B.) (Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia (Mintic),s.f.); que a su vez servirán de base para diligencia el formato FURAG, con el cual las entidades del estado reportaran los avances de la gestión.

En el anexo B, encontraremos cada hoja del instrumento MSPI, así:

Hoja 1 Portada
Hoja 2 Escala de Evaluación
Hoja 3 Levantamiento de la Información
Hoja 4 Áreas involucradas
Hoja 5 Pruebas administrativas
Hoja 6 Pruebas técnicas
Hoja 7 Avance PHVA
Hoja 8 Ciberseguridad
Hoja 9 Madurez MSPI

La Política Nacional de Seguridad Digital-CONPES, este documento fue realizado en el año 2016, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. El documento CONPES 3854 contempla la defensa y seguridad nacional en el entorno digital, la gobernanza, la educación, la regulación, la cooperación internacional y nacional, la investigación y desarrollo. Este documento tiene como población objetivo a los ciudadanos, y todas sus formas de organización. Contiene los antecedentes normativos y de política pública, el marco conceptual, la caracterización y la problemática, la definición, objetivos, estrategias y recomendaciones de la política nacional de seguridad digital. (CONPES & DNP, 2016).

6. ALCANCE Y DELIMITACIÓN DEL PROYECTO

6.1 ALCANCE

Se elaboran las políticas de seguridad, para prevenir los riesgos que se presentan en la manipulación y manejo de información digital específicamente en el grupo de cuentas por pagar del Ministerio de Transporte.

Estos riesgos se presentan cuando tenemos una política de seguridad general, con poca socialización, que además en casi 10 años no ha sido revisada o actualizada.

Inicialmente se realizará una caracterización de la información digital que se maneja en cada una de las bases de datos seleccionadas del Grupo Cuentas por Pagar:

- Relación de pagos
- Administración documental
- Servicios públicos
- Cuentas por pagar

Teniendo en cuenta la norma ISO 12207 sobre ciclos de Ingeniería de Software, se podrán identificar, los riesgos que se presentan en la manipulación de la información digital y aplicar los controles necesarios.

Este proyecto finalizara con el diseñó de un documento digital con la política de seguridad de información para el grupo de Cuentas por Pagar y su respectiva socialización y verificación de cumplimiento.

6.2 DELIMITACIÓN

En el desarrollo del proyecto se realizará una caracterización de la información que se maneja en el Grupo de Cuentas por pagar desde el año 2014, y se hará con observación y encuesta sobre la percepción de seguridad que tienen los funcionarios del grupo, de la información que manipulan a diario.

Se realizará un análisis documental a las políticas de seguridad existente a nivel general en el Ministerio de Transporte desde el año 2008, los modelos que nos presenta el Ministerio de Tecnologías y Comunicaciones, políticas de seguridad del CONPES y la normatividad existente, con el fin de diseñar la política de seguridad del grupo de cuentas por pagar, actualizada y cumpliendo con la normatividad.

El diseño de un documento digital de la política de seguridad de información, será desarrollada específicamente para el Grupo de Cuentas Por Pagar del Ministerio de Transporte, con una temporalidad de revisión anual.

7. METODOLOGÍA

El objeto de este estudio es realizar una investigación aplicada al tema de políticas de seguridad informática para el grupo de Cuentas por Pagar.

- Metodología a utilizar: Se usará metodología descriptiva, explicativa y de observación directa

- Universo o población: Se realizará seguimiento y análisis a cada proceso realizado por los 8 funcionarios del grupo de Central de Cuentas por Pagar.

- Muestras: Se realizará una encuesta a cada uno de los 8 funcionarios del Grupo de Central de Cuentas por Pagar, para conocer la percepción de seguridad de los procesos que cada uno maneja.

- Técnica o instrumentos: Se realizar observación y análisis documental, encuesta y diseño documento.

- Análisis y medición: Esta es una investigación de campo, tomando el estudio de caso real del Grupo de Cuentas por Pagar; el análisis y medición se hará con métodos tanto cualitativos como cuantitativos y con un muestreo probabilístico donde todos los integrantes del grupo de Cuentas por Pagar, podrán informar las formas de ingreso, manipulación y problemáticas presentadas con las bases de datos que a diario utilizan.

Tabla 1. Matriz de metodología.

	Metodología a utilizar	Técnica o instrumentos
Caracterizar la seguridad en la información digital que se maneja en las bases de datos seleccionadas del Grupo Cuentas por pagar: “relación de pagos”, “administración documental” “servicios públicos” y “cuentas pagar”.	Descriptiva Explicativa Observación directa	Observación Encuesta
Analizar situación actual del manejo de la información digital en el Grupo de Cuentas por Pagar e identificar vulnerabilidades y amenazas	Descriptiva, observación directa	Observación
Aplicar el análisis de criterios de las políticas de seguridad de la información digital, al estudio de caso del grupo de Cuentas por Pagar.	Explicativa	Análisis documental
Diseño documento digital con la política de seguridad de la información para el grupo de Cuentas por Pagar	Explicativa	Diseño documental
Fuente: El autor		

8. DESARROLLO DEL PROYECTO

Para la implementación de políticas de seguridad de la información en el grupo de Cuenta por Pagar del Ministerio de Transporte, se han identificado los siguientes activos informáticos:

- Personal
- Equipos de cómputo
- Base de datos Excel y Dbase
- Documentos soporte de las cuentas
- Aplicativo SIIF Nación

Con estos activos se cumplirá con la función del grupo Central de Cuentas por Pagar que es registrar, controlar y alistar todos los pagos que el Ministerio debe realizar a nivel nacional para el cumplimiento de su misión.

Para poder realizar este proceso de pago de cuentas, cada funcionario requiere tener el conocimiento y la experticia necesaria para manejar tanto los equipos como los aplicativos en el cumplimiento de sus funciones.

8.1 CARACTERIZACIÓN RECURSOS DE INFORMACIÓN ADMINISTRADOS POR EL GRUPO DE CUENTAS POR PAGAR

8.1.1 Base de datos relación de pagos

Base de Datos desarrollada en Dbase creado por el Grupo de Informática desde el año 2000.

En esta base de datos, se registran los contratos que el Ministerio de Transporte realiza, objeto, NIT, pagos mensuales, IVA, retenciones, amortizaciones y anticipos hacen parte de esta recopilación de datos; esto se hace con la finalidad de llevar control de los pagos a los contratos y poder realizar las liquidaciones de los contratos con datos confiables

El aplicativo tiene la opción de generación de cuentas por pagar y planillas de cuentas por pagar; pero por lo obsoleto del software no se usa.

El soporte lo realiza el grupo de informática, cuando se presentan problemas.

La ventaja de esta base de datos es que centraliza toda la información de pagos que realiza el ministerio a nivel nacional.

La desventaja se da cuando es manipulada por muchas personas y no se toman las medidas de seguridad pertinentes, poniendo en riesgo la información registrada.

Esta desarrollada en el aplicativo Dbase creado por el Grupo de Informática desde el año 2000, así:

1. El funcionario encargado entra al link de Dbase (menú principal), así:

    - Se encuentran las siguientes opciones:

        MENU GENERAL

        0. TERMINAR
        1. TABLAS
            0. Terminar
            1. Parámetros: en este ítem se pueden modificar los parámetros de la relación de pagos que tiene que ver con fechas de procesos, % IVA, número de planilla, nombre coordinador Grupo Pagaduría, Coordinador Grupo Contabilidad / Coordinador Grupo Central de Cuentas por Pagar y funcionario responsable del Grupo de Contabilidad / Grupo Central de Cuentas por Pagar.

Da la opción de Abandonar o Modificar

2. Bancos
   Terminar
   Adicionar: da la opción de adicionar: código del banco y nombre, digitándolas en los campos correspondientes y al final le dice si desea adicionar el registro o no (s/n).
   Modificar: da la opción de modificar código y nombre del banco. Al final le da opción de grabar o no las modificaciones (s/n)
   De la opción 1 y 2 se sale digitando L
   Eliminar: se puede eliminar digitando código del banco o nombre. Da la opción de eliminar o no (s/n)
   Con enter se sale al menú anterior.
   Consultar: se digita c y le da la opción con llave de digitar código del banco y le despliega el nombre. Si se digita G, despliega el código y el nombre de los bancos registrados.
   Se sale con enter o esc.
3. Terceros: da la opción como en la tabla anterior de adicionar, modificar, eliminar o consultar, los siguientes campos:
   Nit, Nombre o razón social, nombre representante legal, dirección, teléfono, ciudad y cuenta corriente. Con enter se sale.
4. Contratos principales: como en los ítems anteriores da la opción de adicionar, modificar, eliminar o consultar; los siguientes campos:
   Contrato No., año, Nit/cc de tercero, razón social, objeto del contrato, valor contrato sin iva, valor del iva (16%), valor total con iva, porcentaje base iva; se digita (I – Inversión o F – funcionamiento, según el caso). Con enter se sale.
5. Contratos adicionales: igual da las opciones de adicionar, modificar, eliminar y consultar los siguientes campos:
   Contrato principal No., año, contrato adicional No., fecha, valor básico. Se sale con enter
6. Registros presupuestales: da las opciones de adicionar. Modificar, eliminar y consultar los siguientes campos:
   Nro. de registro, fecha, contrato No., Año contrato, beneficiario, valor del contrato, (I/F), dígitos presupuestales y valor. Se sale con esc.

2. CONTRATISTAS

   0. Terminar

1. Saldos: nos muestra los siguientes campos, con la opción de ingresar datos, así:
   Contrato No., año, despliega beneficiario y nit, se digita valor del registro, valor anticipo, valor anticipo especial, valor materia prima, calor contrato.
   Da la opción de grabar datos (s/n)
2. Cuentas: da la opción de terminar; adicionar (se adiciona tramite cuenta contratista); se digita: número de radicación, fecha, número de folios, número contrato, año y sale el beneficiario del contrato, nit, valor del contrato; se digitan: acta, fecha, valor, valor anterior, valor iva, valor anticipo, valor a cobrar próxima cuenta, valor cobrado cuenta anterior, deducciones, amortizaciones, % retención en la fuente, % contribución, multas, concepto; se genera un resumen con: saldo anterior, movimiento y saldo por registro, anticipo, contrato. Da la opción de adicionar o no el registro y con enter terminar.
   Modificar: Con digitar el No. Radicación trae información del contrato y la opción de modificar el campo que se quiera; opción de grabar las modificaciones y dar enter para terminar.
   Eliminar: Con digitar el No. Radicación trae información del contrato y la opción de eliminar y dar enter para terminar.
   Consultar: se puede consultar por código, número de radicación, primero, último, siguiente anterior o con G, despliega información completa de los contratos. Se da enter o esc para salir.
3. Pago cuentas: se digita el número de radicación y año, despliega información del contrato y datos de los pagos, como código del banco, numero de cheque y fecha del pago. Finalmente da la opción de adicionar o no el registro.
4. Informes: en esta parte se pueden imprimir las relaciones de pagos, planillas y contratos.
   0. Terminar

   1. Cuenta de cobro: se digita número de radicación, numero de contrato y año. (No se usa)

   2. Elaboración planilla: la despliega dando la fecha de elaboración

   3. Copia de una planilla: se digita el número de planilla a copiar.

   4. Cuentas, contratos: relación de pagos, digitando número de contrato y año. Da la opción de abandonar, imprimir y enter para terminar.

5. Contratos principales: Se digita el año y saca informe contratos principales del año. Da la opción de abandonar o imprimir.

3. INDEXAR: con enter realiza la actualización.

Terminar y sale del aplicativo.

Esta base de datos de Dbase, lleva más de 10 años en funcionamiento, no se ha actualizado y se han evidenciado algunos problemas como son:

- No tiene ningún tipo de cifrado para su ingreso, si el equipo esta prendido cualquiera accede al link de la base y puede manipularla, modificar o borrar registros.
- Por ser tan antigua y no habérsele realizado modificaciones, para ingresar nuevos registros, toca borrar registros de los primeros años de creación, para que acepte los nuevos.
- Requiere información que no se usa, por ejemplo, pide amortizaciones y anticipos que ya no se realizan.

8.1.2 Base de datos administración documental

Este es un aplicativo de software libre, ORFEO licenciado por GNU/GPL, en el año 2006 y desarrollado e implementado por primera vez en Colombia por la superintendencia de Servicios Públicos Domiciliarios (SSPD). En el año 2008, fue implementado por el Ministerio de Transporte para administrar la documentación interna y externa a nivel nacional.

En el Grupo Central de Cuentas por Pagar, el procedimiento de correspondencia es:

Correspondencia Interna: memorandos u oficios que se generan en el Grupo

- En las plantillas del aplicativo Orfeo se generan los memorandos u oficios que saldrán del grupo.
- Se realiza la radicación correspondiente
- Se imprime el documento y se pasa para firma del coordinador del grupo
- Se genera la planilla para entregar en las ventanillas de correspondencia.
- Se entrega en correspondencia el documento con los soportes si los hubiere y ellos se encargan de hacer la entrega de los memorandos o realizar el envío de los oficios.

Correspondencia externa: Correspondencia que se recibe, de otras dependencias o de fuera del Ministerio.

- Se firma libro de radicación de recibido del Grupo de Correspondencia.
- Firma funcionario que recibió y coloca la fecha de recibido
- Se entrega al Coordinador
- El Coordinador distribuye la correspondencia, según el tema a los funcionarios del grupo.
- Cada funcionario realizara el trámite correspondiente y devuelve al Coordinador quien realiza el respectivo descargue en Orfeo, excepto los radicados de servicios públicos que se reasigna por Orfeo a la persona encargada de pagos servicios públicos y la misma realiza el descargue correspondiente.

En el grupo de Central de Cuentas cada funcionario ingresa al aplicativo Orfeo, con el mismo usuario y clave con que se ingresa a equipo.

Todos los permisos con que cuenta el aplicativo los tiene solo el Coordinador, pero el proporciona su usuario y clave a otros funcionarios del grupo, para que puedan ayudar en el descargue, radicación, asignación y devoluciones de correspondencia, que surja en el proceso.

El aplicativo permite acceso a estadísticas de.

- radicados en la dependencia
- radicados por funcionario (pendientes por rango de fecha)
- radicados tramitados
- radicados devueltos

Esta base de datos fue realizada en software libre, tiene mucha aplicabilidad y está en constante actualización, por parte de los ingenieros de sistema del Grupo de Informática.

Como es un aplicativo al cual tienen acceso todos los funcionarios del Ministerio, debe cuidarse mucho la seguridad. El mayor problema de seguridad que se encuentra en este aplicativo, es que los coordinadores o directivos; facilitan sus claves a otros funcionarios para que trabajen, desde su perfil y tanto los directivos como los coordinadores tienen todos los permisos y accesos habilitados.

8.1.3 Base de datos servicios públicos

Base de datos en Excel, creada desde el año 2007, con combinación de correspondencia en formatos Word. En esta base de datos se realiza la liquidación y control de los pagos de servicios públicos a nivel nacional.

Procedimiento

1. Se recibe de correspondencia, la factura de servicio público
2. Se clasifica si es servicio público de planta central Bogotá, se cancela por orden de pago DOC = OBLIG si es de Direcciones Territoriales o Inspecciones Fluviales DOC = CM, así:

    - Se mira en la base de datos cual fue el último pago realizado, de la factura y cuenta recibida.
    - Se verifica código de cuenta, numero de factura, valor y periodo a cancelar.
    - La base de datos tiene los siguientes campos a llenar:
        REG: número de consecutivo en la base
        DOC: Si es caja menor (CM), si es obligación (OBLIG)
        NUMERO: número de OBLIG o CM
        DIA: día de registro en base de datos
        MES: mes de registro en base de datos
        DOC ANTERIOR: número de CM u OBLIG del último pago
        ANT DESDE: periodo del último pago desde
        ANT HASTA: periodo del último pago hasta
        ID SEDE: Si es planta central PC
        Si es Inspección Fluvial IF

Si es Dirección Territorial DT
NOMBRE SEDE: nombre de la sede, si es IF el nombre, si es DT el departamento y si es PC sedes Bogotá.
NIT: NIT de la empresa beneficiaria
BENEFICIARIO: Nombre de la empresa prestadora del servicio
ASEO: Se digita el valor correspondiente a aseo
CONSUMO ASEO (mts 3): Se digita el consumo
COSTO UNIDAD ASEO: Si la factura lo tiene se digita el costo unidad
AC y AL: Se digita el valor de acueducto y alcantarillado
CONSUMO AC Y AL (mt3): Se digita el consumo
AC AL Y AS: Se digita el valor de acueducto alcantarillado y aseo
CONSUMO AC AL AS (mts3): se digitan el consumo
COSTO UNIDAD AC AL Y AS: se digita el costo de la unidad
TOTAL AC AL AS: Se suma valor a pagar aseo acueducto y alcantarillado
ENERGIA: Se digita el valor de energía
CONSUMO ENERGIA (KWH): Se digita el consumo de energía
COSTO UNIDAD ENERGIA: Se digita el costo unidad energía
TELEFONO: Se digita el valor de teléfono
CONSUMO TELEFONO (min): se digita el consumo
COSTO UNIDAD TELEFONO: se digita el costo unidad
T CELULAR: se digita el valor de celular
CONSUMO CELULAR (min): se digita el consumo celular
COSTO UNIDAD CELULAR: se digita el costo unidad
GAS NATURAL: se digita el valor de gas
CONSUMO GAS NATURAL (mts3): se digita el consumo
COSTO UNIDAD GAS: se digita el costo unidad
INTERNET: se digita el valor de internet
CONSUMO INTERNET (min): se digita el consumo
COSTO UNIDAD INTERNET: se digita el costo unidad
TOTAL: Se hace la sumatoria total
EN LETRAS: Se digita el valor en letras
DESDE: periodo inicial del consumo
HASTA: periodo final del consumo
VENCE EN: fecha de vencimiento factura
DETALLE FACTURAS: número de facturas cuentas, contrato o código de identificación
0352-: Casilla en blanco
BANCO: nombre entidad bancaria del pago
CUENTA No.: Número de cuenta bancaria
CLASE: corriente o de ahorros

DOCUMENTO: si es original o copia de la factura
FECHA DOC: fecha de emisión de la factura
OBSERVACIONES: Se digitan observaciones si es pertinente
RAD CUC: número radicado Orfeo
RECIBIDO EL: fecha de recibido el radicado o email
LIQUIDO: nombre de la persona que liquida
ELABORO: nombre de la persona que elabora el pago.

3. Una vez realizada la liquidación, se guardan los cambios y se cierra la base de datos, se ingresa a archivo Word de combinación de correspondencia, para imprimir la liquidación; según el caso archivo para CM y archivo para OBLIG.
4. Si es obligación se sacan dos copias y se arman 2 paquetes uno para pagaduría y otro para el archivo de central de cuentas. Si es CM se arman 3 paquetes, uno consecutivo, otro para soportes del reembolso y el de archivo del grupo.
5. Las cuentas que son por obligación se relacionan en un cuadro control y se entregan en el grupo presupuesto, quienes realizan el registro presupuestal. Una vez las devuelve presupuesto, se ingresa al Sistema de Información Financiera de la Nación (SIIF) y se procede a realizar la cuenta por pagar y la obligación; se pasan los documentos a la persona encargada de la base de datos de control de cuentas quien la ingresa la información en la base y elabora la planilla que se pasara al Grupo de Pagaduría, donde finalmente se realiza el pago o transferencia bancaria pertinente.
6. Las cuentas que son para pago por caja menor, se realiza el trámite de transferencia electrónica empresarial de Davivienda a cada cuenta.
7. Se hace el registro de cada pago por caja menor en SIIF
8. Una vez se ha realizado el pago ya sea por obligación o por caja menor y se tienen los soportes de pago correspondientes se procede a reportar los pagos a cada empresa, Dirección Territorial o Inspección Fluvial, para que sean aplicados.
9. Se deben tener conciliación entre los saldos SIIF caja menor y saldos en la cuenta bancaria de Davivienda.
10. Se descarga del aplicativo de correspondencia y se archivan los documentos soportes.

Esta base de datos solo está en un computador del grupo de cuentas por pagar y está a cargo de una sola persona y está hecha en Excel, no tiene ningún tipo de seguridad, la persona que ingrese al computador donde se maneja, puede manipularla libremente; el computador donde está, debe estar todo el tiempo encendido, pues en él está la conexión de la impresora en red de todo el grupo.

8.1.4 Base de datos control cuentas por pagar

Base de datos realizada en Excel, desde el año 2010, se registran todas las cuentas que se pasan a pagaduría para el pago final.

Se pasan cuentas de:

Administración	Ayuda educativa	Caja menor
Capacitación	Chatarrización	Contratos
Cuotas partes pensiónales	Impuestos	Nomina
Proveedores	Prestaciones sociales	Seguros / pólizas
Sentencias	Servicios públicos	Trasteo funcionarios
Viáticos	Pago contratistas	Pago Proveedores
Pago Arriendos	Pago Administraciones	Pago serv. Públicos
Pago sentencias	Pago conciliaciones	Pago Nomina
Pago ayudas educativas	Pago viáticos	Pago Chatarrización

Procedimiento:

La persona encargada de la base de datos recibe las obligaciones presupuestales con los documentos soportes, digita en la base de datos los siguientes campos

GESTION: código unidad ejecutora de SIIF

24-01-01-000 Gastos generales
24-01-01-001 UMUS
24-01-01-002 Sobretasa a la gasolina
24-01-01-004 PVR
24-01-01-005 RUNT
24-01-01-006 Seguridad Vial
24-01-01-007 Logística
24-01-01-008 Cooperación Internacional
REGALIAS

CONCEPTO: qué clase de pago es: admón., ayuda educativa, caja menor, capacitación funcionarios, carta aceptación, Chatarrización, contrato, cuotas partes pensiónales, impuestos, nomina, orden de compra, prestaciones sociales, profesionalización (universidad funcionarios), resolución, seguros/pólizas, sentencias, servicios públicos, trasteos funcionarios, viáticos

TIPO CONCEPTO: Según el concepto puede ser: acueducto, apertura caja menor, arrendamiento, arrendamiento bienes inmuebles, aseo, autorización viáticos, celular, combustible, consultoría, energía, estimulo educativo, regalías, gas, haberes laborales, interadministrativo, nomina general, nomina pensionados, obra, otros servicios públicos, placas, predial, prestación servicios, reembolso, registro presupuestal, suministro, suscripciones, teléfono, fax y otros, vehículos, vigilancia.
NUMERO: Numero del tipo de concepto, puede ser numero de contrato, de caja menor, carta aceptación, orden de compra, placa, registro presupuestal.
NIT/CC: nit o cedula del beneficiario
BENEFICIARIO: nombre de la empresa o persona natural beneficiaria del pago
VALOR: valor a pagar
DETALLE: periodo de pago
ACTA No.: Número del acta para contratistas
DOCUMENTO SOPORTE COBRO: Cuenta de cobro, factura, nomina, reporte impuesto predial, resolución.
No. DOCUMENTO: número de documento del soporte de cobro
RADICADO ORFEO: número de radicado Orfeo
FECHA RADICADO ORFEO: fecha de radicado Orfeo
FECHA RECIBIDO CENTRAL DE CUENTAS fecha de recibido en central de cuentas
FECHA REVISION CXP: fecha de revisión por funcionario de central de cuentas
OBSERVACIONES REVISION CXP: se hace la observación si se debe corregir algo o se da OK si no hay correcciones
FECHA RECIBIDO CORRECION EN CXP Y/O PAZ Y SALVO: fecha de recibo soportes con correcciones
FECHA DISPONIBLE DE PAC/RECIBO RP PPTO: fecha del plan anual de caja / recibo registro presupuestal
FECHA DE PAGO: Fecha de pago, figura en la obligación SIIF
VIGENCIA: año de la vigencia actual o año anterior
CXP No.: Numero de la cuenta por pagar
FECHA CXP: Fecha de la cuenta por pagar
OBLIGACION No.: número de la obligación SIIF
FECHA OBLIGACIÓN: fecha de la obligación SIIF
CONSECUTIVO PLANILLA PAGADURIA: número consecutivo de la planilla de entrega de cuentas al Grupo de Pagaduría.
FECHA PLANILLA PAGADURIA: Fecha de la planilla de pagaduría.

Esta base de datos está en red con cada uno de los funcionarios del grupo de cuentas por pagar. El grupo de informática tiene ingreso para realizar backup.

Aunque cada funcionario tiene acceso a la base de datos, está destinada para consulta y solo una persona se encarga de alimentarla.

No hay clave de acceso a la base de datos, con solo abrir el computador ya se puede ingresar al link de la base.

La única restricción es que solo un usuario puede hacer modificaciones, es decir si un segundo usuario ingresa simultáneamente solo le permita lectura mas no modificación.

Estas bases de datos de servicios públicos y control cuentas por pagar están hechas en Excel, se cierra a final de año y se da apertura a un nuevo archivo para cada año.

Estas cuatro bases de datos, deben tener un cifrado especial, pues tienen información importante de los pagos que se realizan a nivel nacional a proveedores, contratista y entidades de servicios públicos.

Sobre todo, se deben dar las pautas a cada integrante del grupo para mantener un manejo adecuado, consiente y seguro de la información.

8.2 RECOLECCION DE INFORMACIÓN SOBRE SEGURIDAD INFORMATICA EN EL GRUPO DE CUENTAS POR PAGAR

Con el fin de verificar la seguridad de la información en el Grupo de Cuentas por Pagar, se realiza una encuesta a los 8 funcionarios del grupo; para hacer un estudio cuantitativo y cualitativo de la situación.

Estructura de la encuesta a realizar a los funcionarios del grupo de Cuentas por Pagar

Manejo de la información de los funcionarios

1. Considera que la base de datos de control de cuentas cumple con las funciones de forma

a. Completa
b. Incompleta
c. No la usa

2. Conoce o ha realizado la eliminación de campos o información de otros registros.
    a. Si
    b. No
    c. No la usa

3. Considera que la base de datos de Dbase para relación de pago, cumple con las funciones para las que fue creada
    a. Si
    b. No
    c. No la usa

4. Considera que la base de datos de servicios públicos se puede modificar para hacerla más funcional
    a. Si
    b. No
    c. No la usa

5. Considera que el aplicativo Orfeo, cumple con las funciones de administración documental, definidas en los procedimientos del grupo
    a. Si
    b. No
    c. No la usa

6. Con que frecuencia accede a la base de datos de control de cuentas
    a. Una vez al día
    b. Más de una vez al día
    c. No la usa

7. Con que frecuencia accede a la base de datos de servicios público
    a. Una vez al día
    b. Más de una vez al día
    c. No la usa

8. Con que frecuencia accede a la base de datos de Dbase relación de pagos
    a. Una vez al día
    b. Más de una vez al día
    c. No la usa

9. Con que frecuencia accede al aplicativo Orfeo
    a. Una vez al día

b. Más de una vez al día
c. No la usa

10. Considera que el acceso a las bases de datos que utiliza en el grupo Central de Cuentas por Pagar es:
    a. Fácil
    b. Difícil
    c. No la usa

11. Cómo considera el nivel de seguridad, para el ingreso a la base de datos de control de cuentas
    a. Seguro
    b. Inseguro
    c. No sabe

12. Como considera el nivel de seguridad, para el ingreso a la base de datos de servicios públicos
    a. Seguro
    b. Inseguro
    c. No sabe

13. Como considera el nivel de seguridad para el ingreso a la base de datos de relación de pagos
    a. Seguro
    b. Inseguro
    c. No sabe

14. Como considera el nivel de seguridad, para el ingreso al aplicativo Orfeo
    a. Seguro
    b. Inseguro
    c. No sabe

15. Qué nivel de seguridad considera que debe tener el acceso a las bases de datos que se manejan en el grupo Central de Cuentas por Pagar.
    a. Alto
    b. Medio
    c. No sabe

Se Aplicó la encuesta a ocho funcionarios en el grupo central de cuentas, con los siguientes resultados:

Tabla 2. Análisis encuesta

Encuesta Política de Seguridad de Información Digital Grupo Cuentas por Pagar Ministerio de Transporte												
No.	**Pregunta**	**Respuesta**	**Jesus**	**Olga**	**Yeni**	**José David**	**Daniela**	**Ivonne**	**Luz Mila**	**Ligia**	**Frecuencia Absoluta**	**Frecuencia Relativa**
1	Considera que la base de datos de control de cuentas cumple con las funciones de forma	Completa	1	1	1	0	0	0	0	1	4	50,00%
		Incompleta	0	0	0	1	1	1	1	0	4	50,00%
		No la usa	0	0	0	0	0	0	0	0	0	0,00%
2	Conoce o ha realizado la eliminación de campos o información de otros registros	Si	0	1	1	0	0	1	1	0	4	50,00%
		No	1	0	0	1	1	0	0	1	4	50,00%
		No la usa	0	0	0	0	0	0	0	0	0	0,00%
3	Considera que la base de datos de Dbase para relación de pago, cumple con las funciones para las que fue creada	Si	1	1	0	0	0	0	0	1	3	37,50%
		No	0	0	0	1	1	1	0	0	3	37,50%
		No la usa	0	0	1	0	0	0	1	0	2	25,00%
4	Considera que la base de datos de servicios públicos se puede modificar para hacerla más funcional:	Si	1	0	0	1	1	1	0	0	4	50,00%
		No	0	0	0	0	0	0	0	0	0	0,00%
		No la usa	0	1	1	0	0	0	1	1	4	50,00%

Tabla 2. (Continuación)

5	Considera que el aplicativo Orfeo, cumple con las funciones de administración documental, definidas en los procedimientos del	Si	1	1	0	1	1	0	1	1	6	75,00%
		No	0	0	0	0	0	1	0	0	1	12,50%
		No la usa	0	0	1	0	0	0	0	0	1	12,50%
6	Con qué frecuencia accede a la base de datos de control de cuentas:	Una vez al día	0	0	0	0	0	0	0	0	0	0,00%
		Más de una vez al día	0	1	1	1	1	1	1	1	7	87,50%
		No la usa	1	0	0	0	0	0	0	0	1	12,50%
7	Con qué frecuencia accede a la base de datos de servicios públicos:	Una vez al día	0	0	0	0	1	0	0	0	1	12,50%
		Más de una vez al día	0	0	0	1	0	1	0	0	2	25,00%
		No la usa	1	1	1	0	0	0	1	1	5	62,50%
8	Con qué frecuencia accede a la base de datos de Dbase relación de pagos:	Una vez al día	0	0	0	0	0	0	0	1	1	12,50%
		Más de una vez al día	1	1	0	1	1	1	0	0	5	62,50%
		No la usa	0	0	1	0	0	0	1	0	2	25,00%
9	Con qué frecuencia accede al aplicativo Orfeo:	Una vez al día	0	0	0	0	0	0	0	0	0	0,00%
		Más de una vez al día	0	1	0	1	1	1	0	1	5	62,50%
		No la usa	1	0	1	0	0	0	1	0	3	37,50%

Tabla 2. (Continuación)

10	Considera que el acceso a la base de datos que utiliza en el grupo central de cuentas por pagar es:	Fácil	1	1	1	0	1	0	1	1	6	75,00%
		Difícil	0	0	0	1	0	1	0	0	2	25,00%
		No la usa	0	0	0	0	0	0	0	0	0	0,00%
11	Cómo considera el nivel de seguridad, para el ingreso a la base de datos de control de cuentas:	Seguro	0	1	1	0	0	0	0	1	3	37,50%
		Inseguro	1	0	0	1	1	1	1	0	5	62,50%
		No sabe	0	0	0	0	0	0	0	0	0	0,00%
12	Cómo considera el nivel de seguridad, para el ingreso a la base de datos de servicios públicos:	Seguro	1	0	0	0	0	0	0	0	1	12,50%
		Inseguro	0	0	0	1	1	1	0	1	4	50,00%
		No sabe	0	1	1	0	0	0	1	0	3	37,50%
13	Cómo considera el nivel de seguridad para el ingreso a la base de datos de relación de pagos:	Seguro	1	1	0	0	0	0	0	1	3	37,50%
		Inseguro	0	0	0	1	1	1	0	0	3	37,50%
		No sabe	0	0	1	0	0	0	1	0	2	25,00%
14	Cómo considera el nivel de seguridad, para el ingreso al aplicativo Orfeo:	Seguro	1	1	1	1	0	0	1	1	6	75,00%
		Inseguro	0	0	0	0	1	1	0	0	2	25,00%
		No sabe	0	0	0	0	0	0	0	0	0	0,00%

Tabla 2. (Continuación)

15	Qué nivel de seguridad considera que debe tener el acceso a las bases de datos que se manejan en el grupo central de cuentas por pagar:	Alto	0	1	0	1	1	1	1	1	6	75,00%
		Medio	1	0	1	0	0	0	0	0	2	25,00%
		No sabe	0	0	0	0	0	0	0	0	0	0,00%
Fuente: El autor												

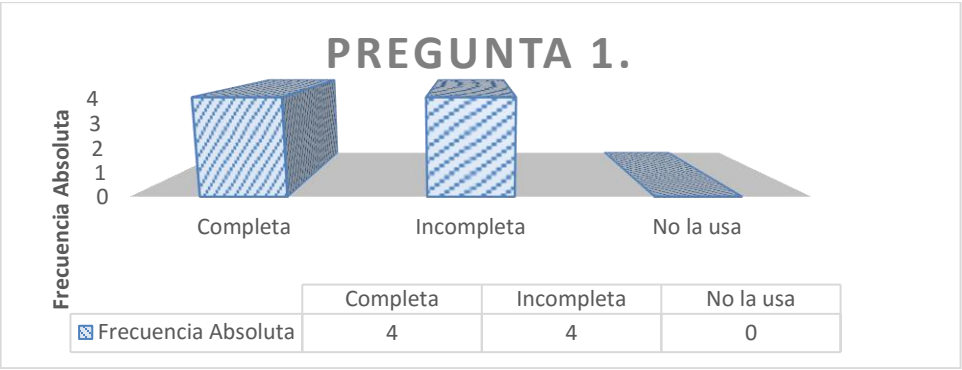
Conclusiones encuesta:

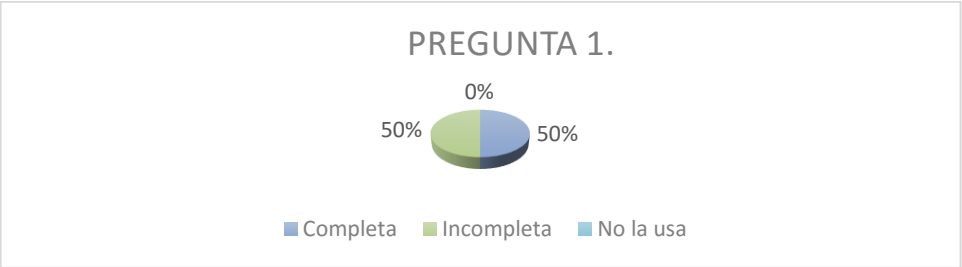
En términos generales se evidencia que la base de datos que más funcionarios usan es la de control de cuentas por pagar que a su vez es la más insegura.

La mayoría de funcionarios del grupo de cuentas por pagar, coincidieron en que el manejo de todas las bases de datos, deben ser más seguras.

Analizando pregunta por pregunta, tenemos:

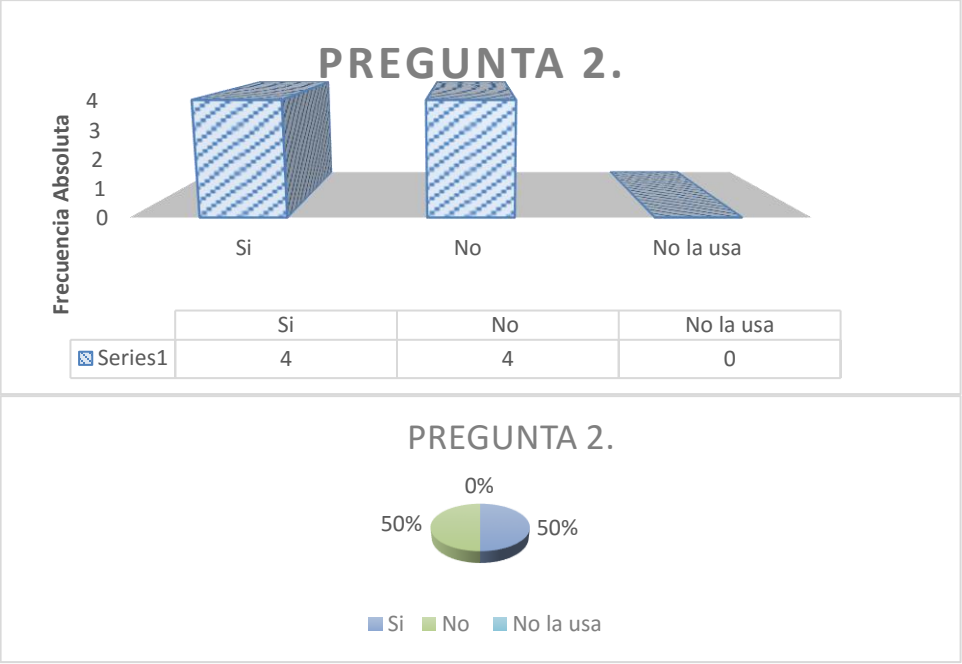
Ilustración 2. Análisis grafico pregunta 1





Fuente: El autor

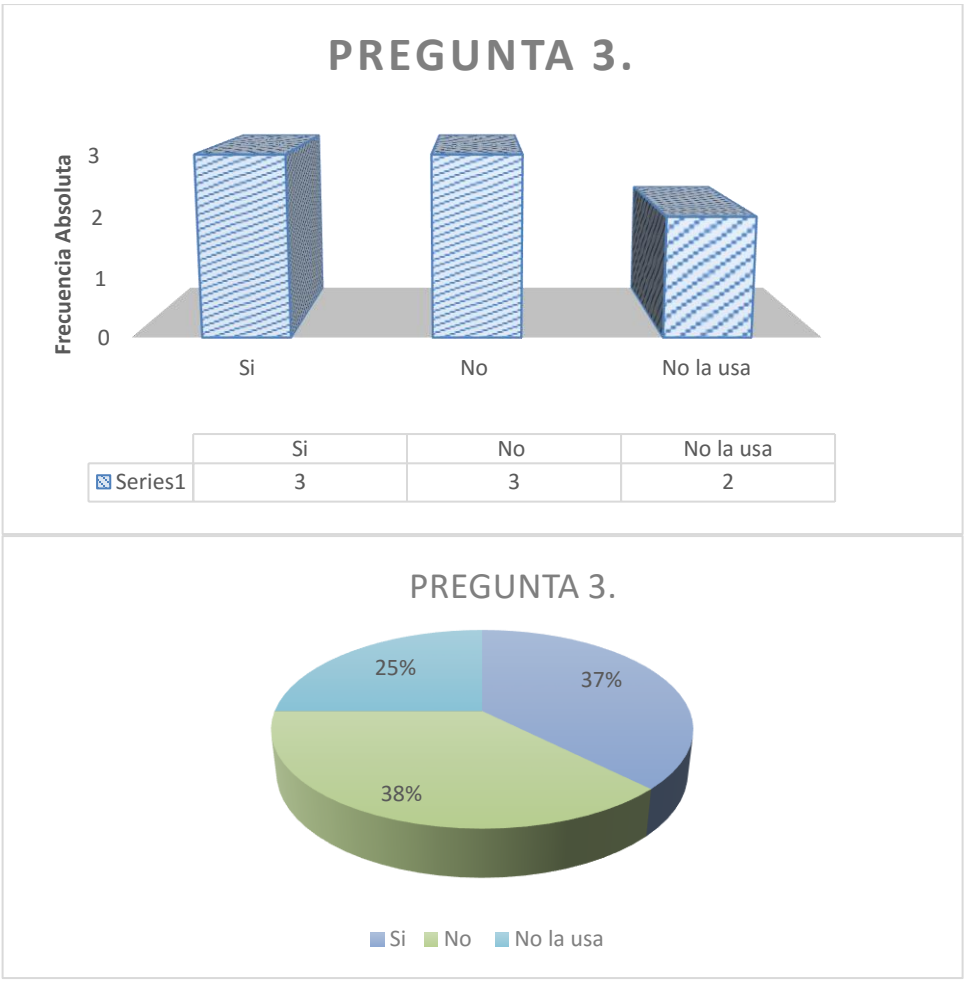
Ilustración 3. Análisis grafico pregunta 2



Fuente: El autor

Los funcionarios del grupo de cuentas por pagar, tienen opinión dividida en la funcionalidad de la base de datos de control cuentas por pagar.

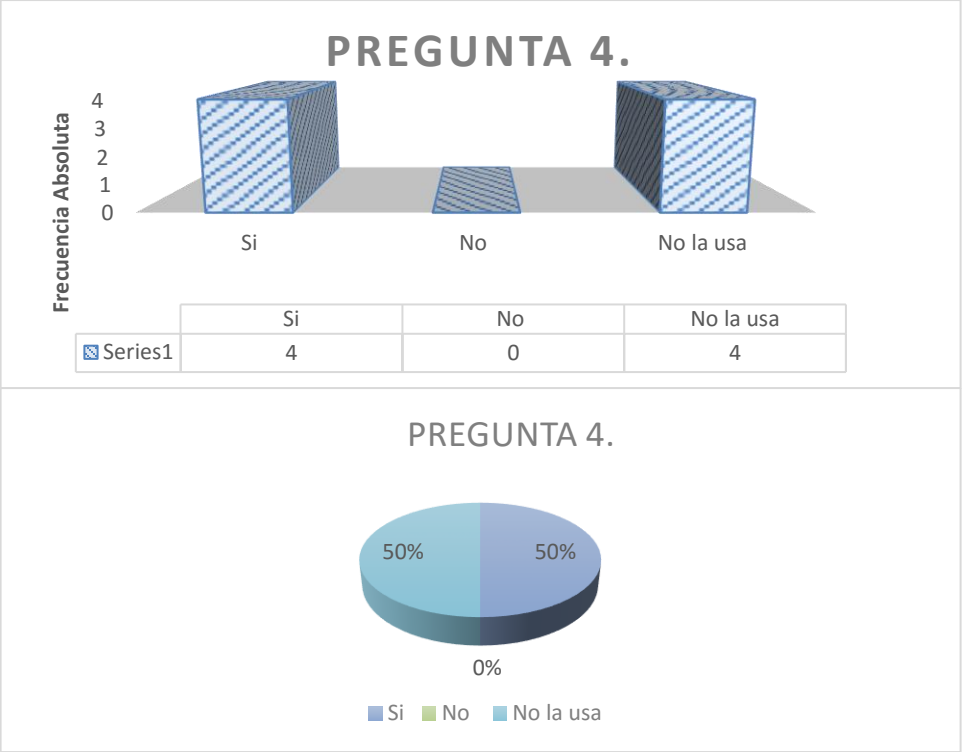
Ilustración 4. Análisis grafico pregunta3



Fuente: El autor

Para la mayoría de encuestados no es funcional la base de datos de Dbase de relación de pagos.

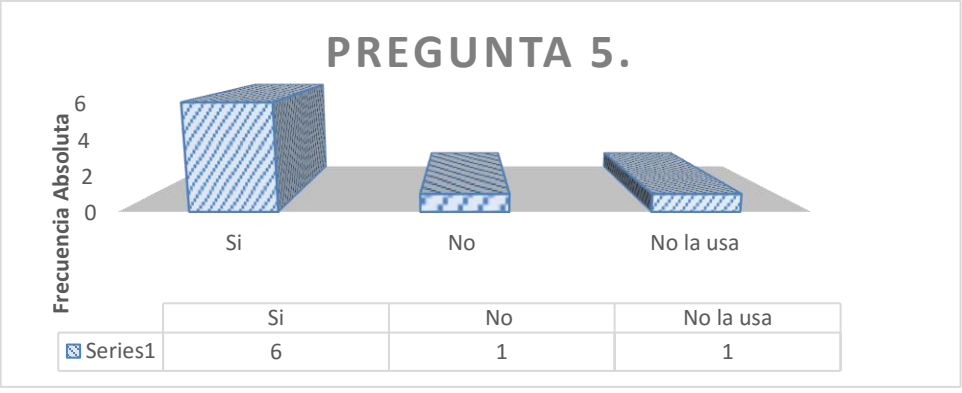
Ilustración 5. Análisis grafico pregunta 4

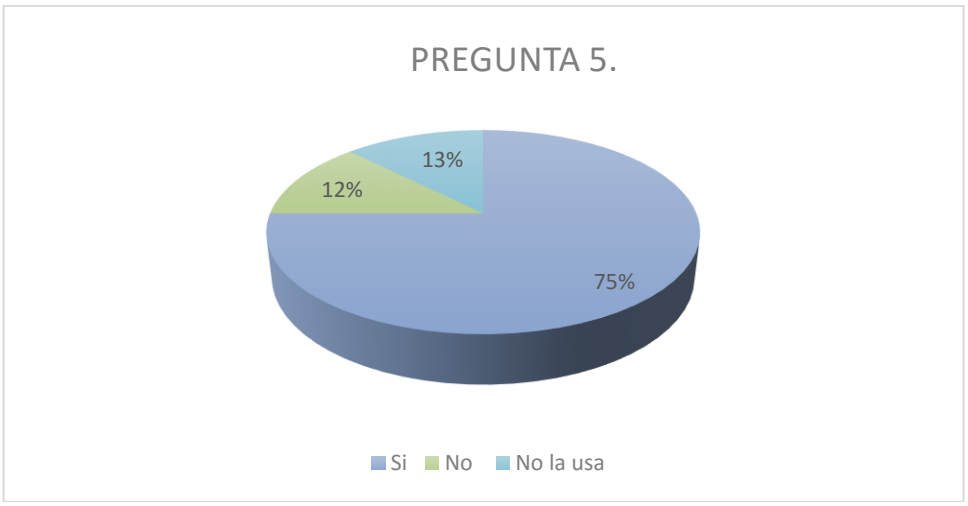


Fuente: El autor

Esta base de datos en términos generales solo es usada por un funcionario, y la percepción es que debe hacérsele ajustes para obtener mejores resultados.

Ilustración 6. Análisis grafico pregunta 5

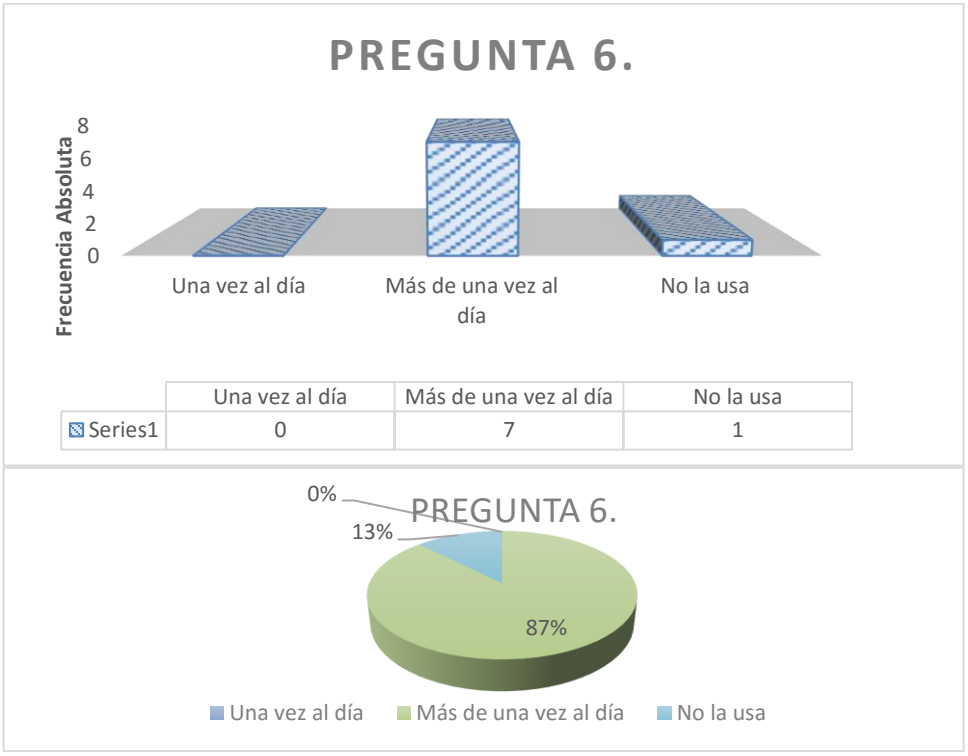




Fuente: El autor

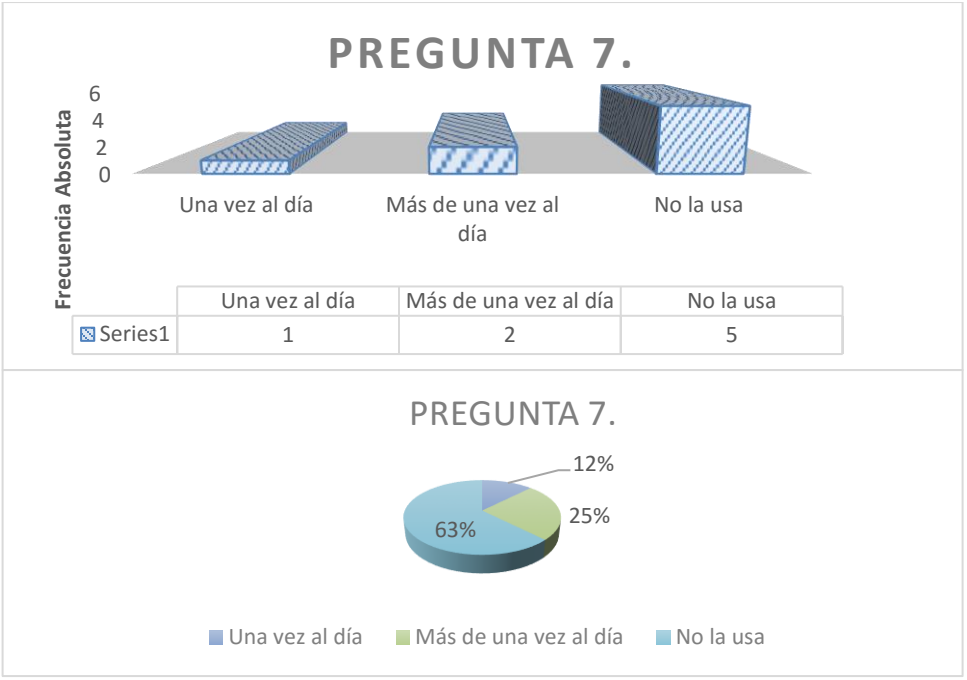
La mayoría de encuestados cree que el aplicativo Orfeo es funcional para la administración documental.

Ilustración 7. Análisis grafico pregunta 6



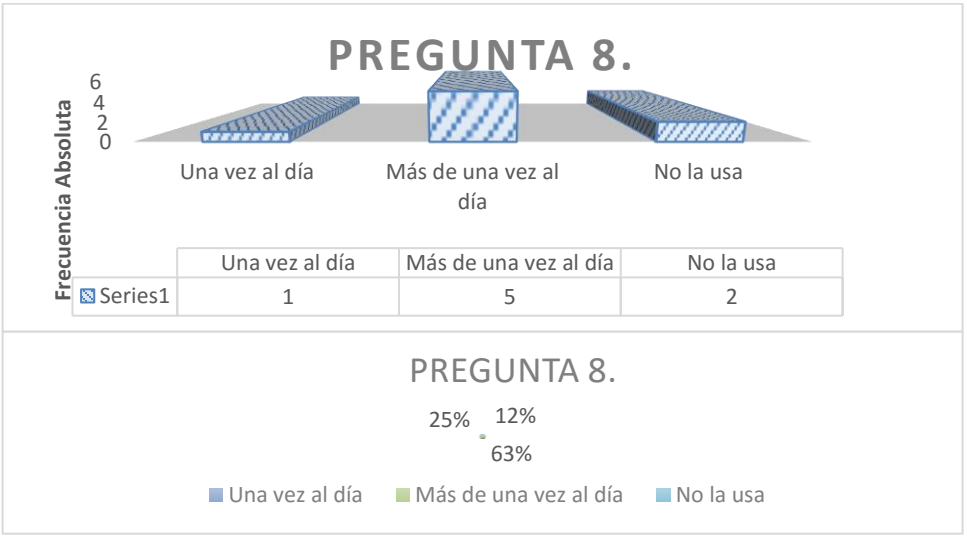
Fuente: El autor

Ilustración 8. Análisis grafico pregunta 7



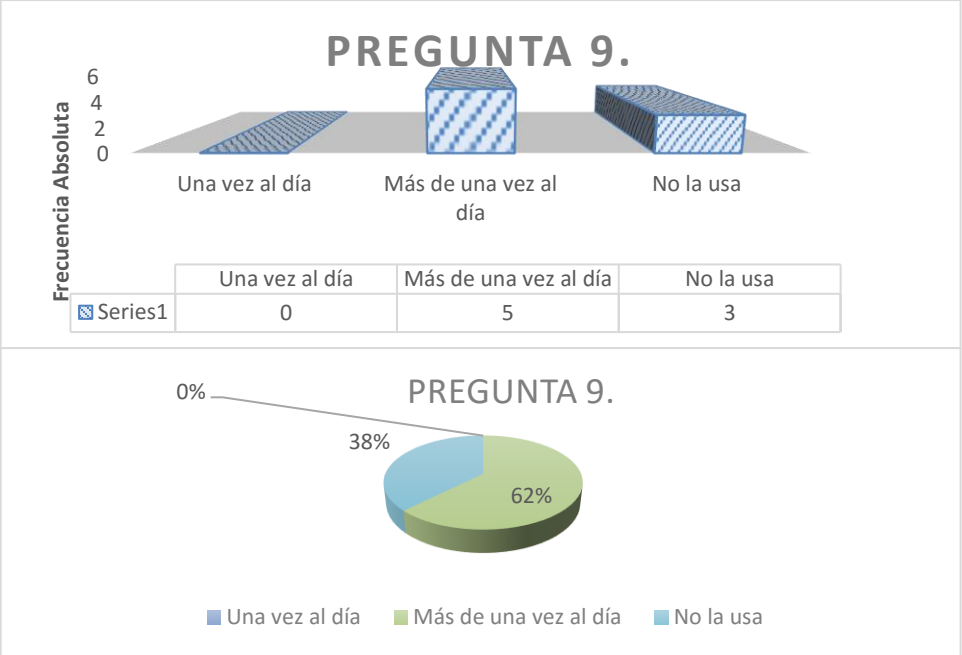
Fuente: El autor

Ilustración 9. Análisis grafico pregunta 8



Fuente: El autor

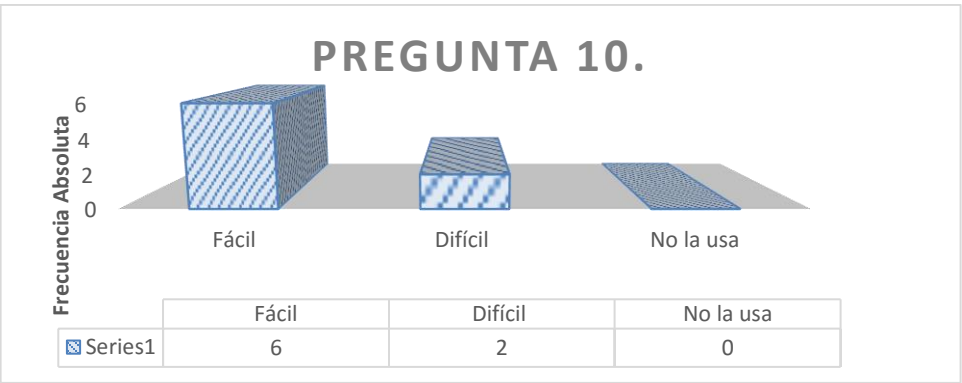
Ilustración 10. Análisis grafico pregunta 9

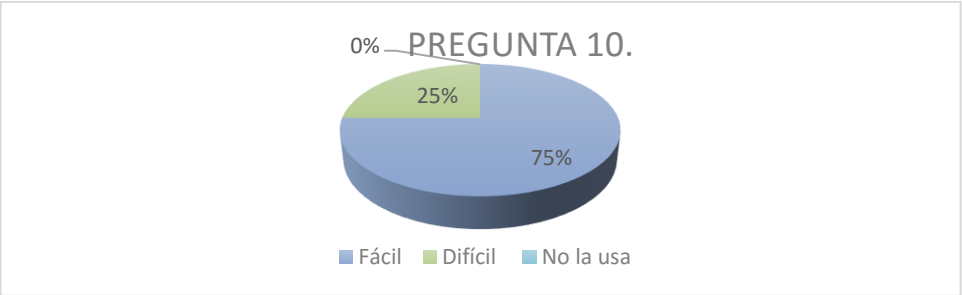


Fuente: El autor

La base de datos que con más frecuencia se usa es la de Control Cuentas por Pagar y el aplicativo Orfeo.

Ilustración 11. Análisis grafico pregunta 10

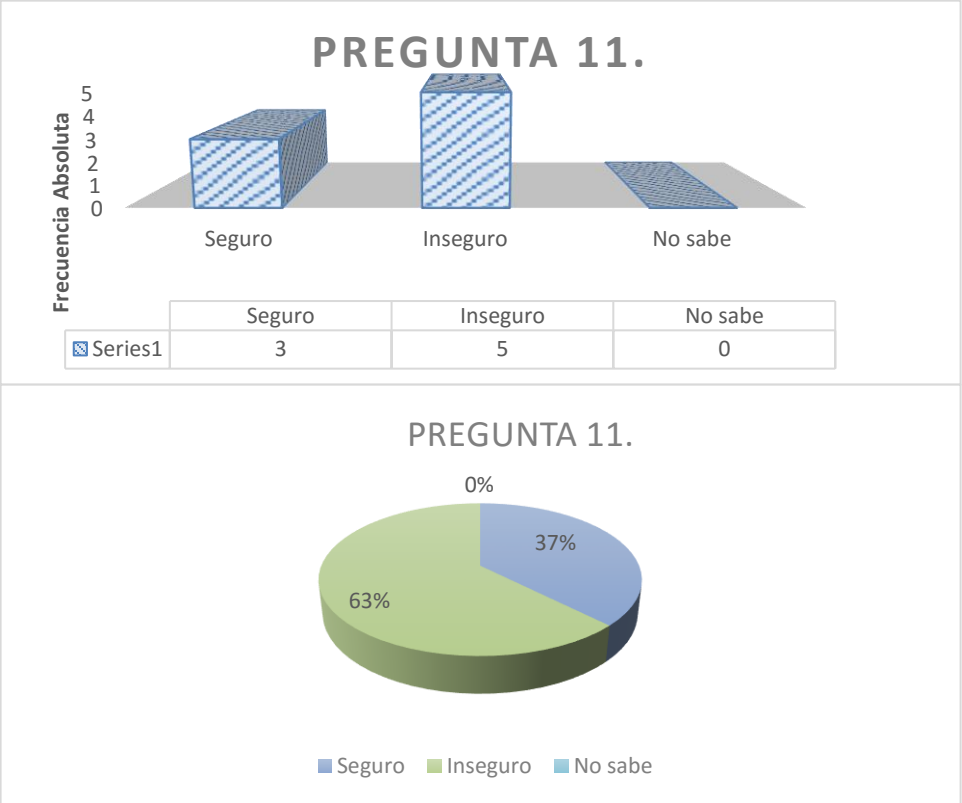




Fuente: El autor

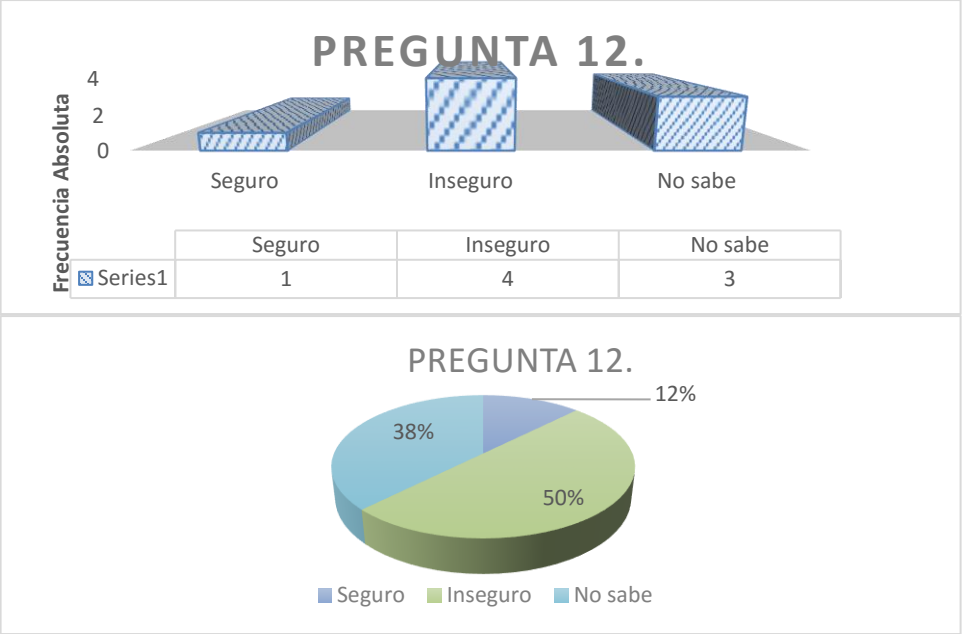
La mayoría de funcionarios del grupo accede con facilidad a la base de datos de control cuentas por pagar.

Ilustración 12. Análisis grafico pregunta 11



Fuente: El autor

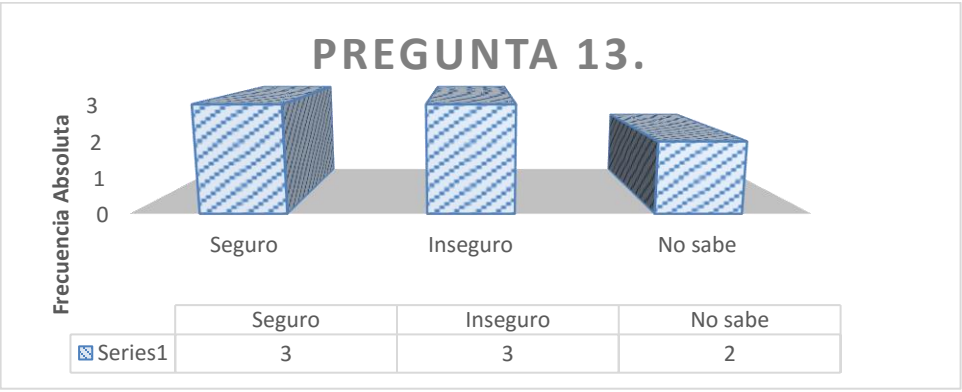
Ilustración 13. Análisis grafico pregunta 12

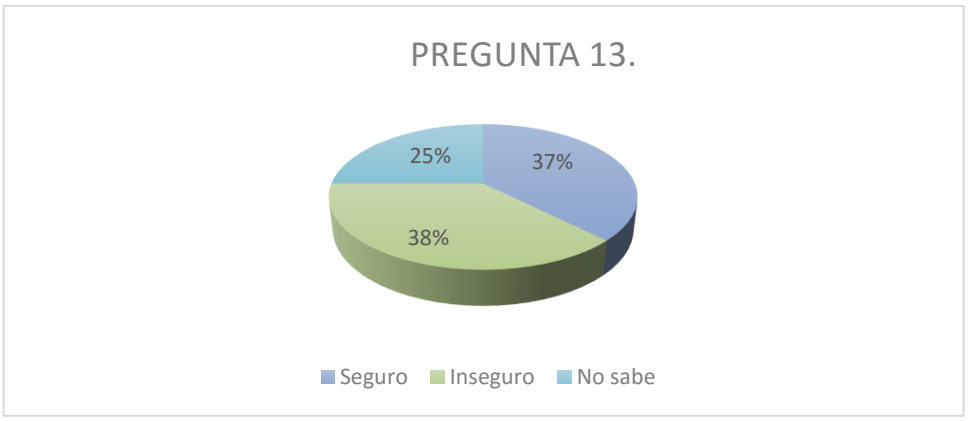


Fuente: El autor

La mayoría de funcionarios está de acuerdo en que el acceso a la base de datos de control de cuentas por pagar y la de servicios públicos es inseguro.

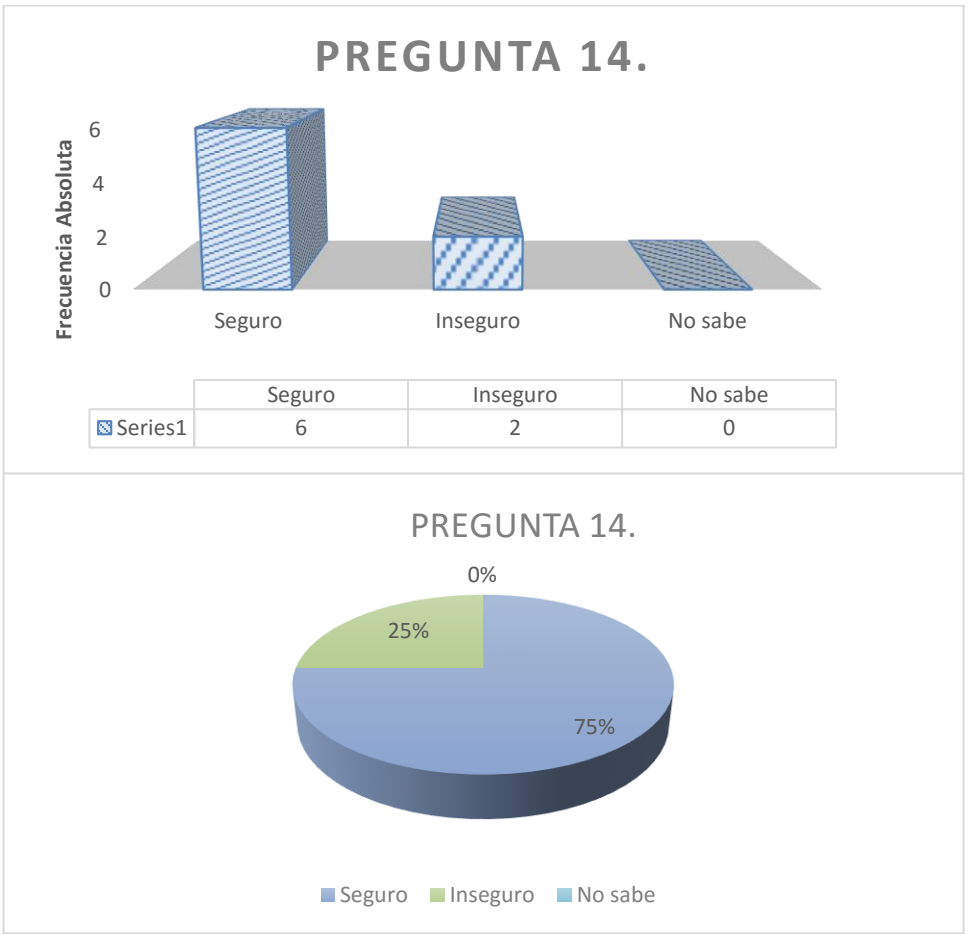
Ilustración 14. Análisis grafico pregunta 13





Fuente: El autor

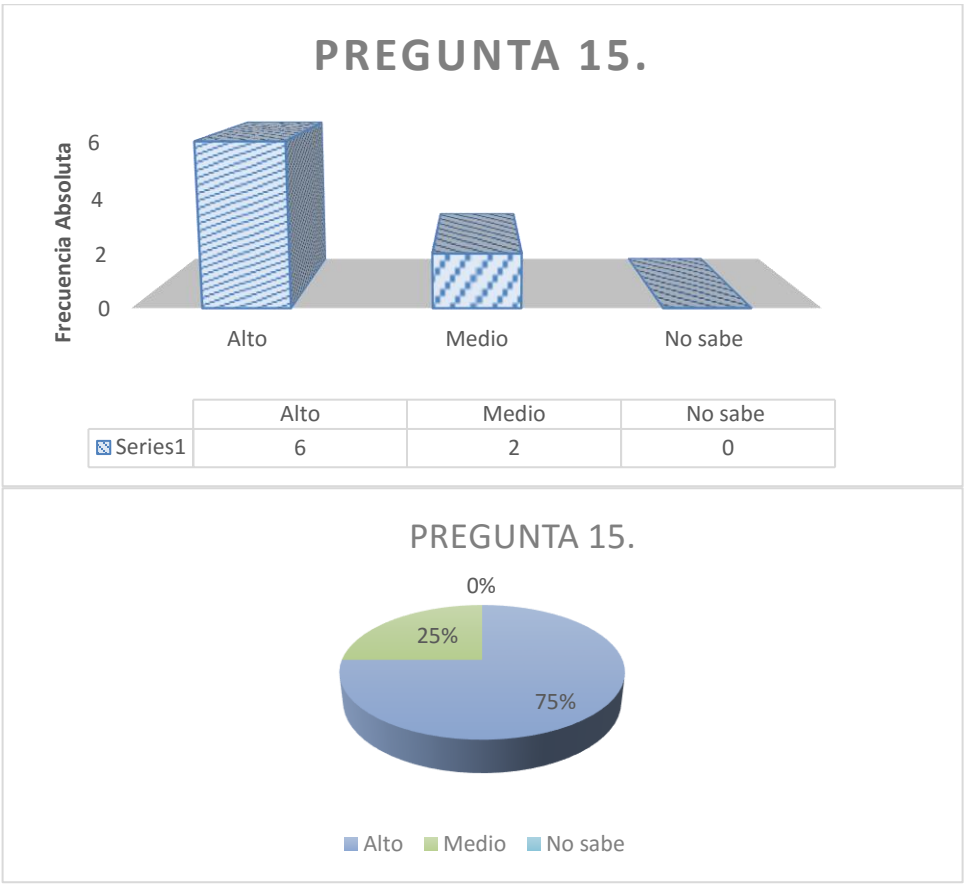
Ilustración 15. Análisis grafico pregunta 14



Fuente: El autor

En cuanto a la base de datos de relaciones de pago tiene un nivel de inseguridad estable y el aplicativo Orfeo, si creen que es seguro.

Ilustración 16. Análisis grafico pregunta 15



Fuente: Autor

La mayoría de funcionarios del grupo de cuentas por pagar, coinciden en que se debe dar un nivel de acceso alto a las 4 bases de datos que se utilizan.

Por el análisis anterior, se determina que es conveniente y prioritario la aplicación de políticas de seguridad en el manejo de la información que se manipula en el grupo de cuentas por pagar.

9. ANALISIS SITUACION ACTUAL DEL MANEJO DE LA INFORMACIÓN DIGITAL EN EL GRUPO CENTRAL DE CUENTAS POR PAGAR

9.1 SITUACIÓN ACTUAL

El grupo de Central Cuentas por Pagar, se encarga del proceso de liquidar todos los pagos a funcionarios, registros y comprobantes para cada pago en el SIIF, alimentar la base de datos de control de cuentas por pagar ingresando información desde el momento en que se recibe de correspondencia hasta el momento en que se entrega al grupo de pagaduría para su respectivo desembolso y posteriormente el descargue en Orfeo. Este proceso se hace para los pagos de nómina, haberes, sentencias, conciliaciones y viáticos de los funcionarios; pagos y viáticos de contratistas, pagos proveedores y pagos desintegración vehicular.

Se encarga también de liquidar y realizar el pago de los servicios públicos a nivel nacional por medio de caja menor; liquidar y dejar listo los pagos de servicios públicos de planta central. Para el control y liquidación se usa la base de datos de servicios públicos, alimentándola desde el momento en que ingresa la factura por correspondencia o por correo electrónico hasta el archivo en el sistema de administración documental. Paralelo al trámite de pago y registro en la base de datos se debe hacer conciliación con el banco donde se realizan las transferencias electrónicas del pago y registro en SIIF, esto para los pagos de Direcciones Territoriales e Inspecciones Fluviales. En planta central se liquida, se radica y obliga en el aplicativo SIIF hasta que sale a Pagaduría para el desembolso.

La base de datos de relación de pagos, es una base de ayuda, para tener constancia cuántos contratos hay en determinado momento, montos, plazos y pagos realizados y pendientes; Es indispensable para la liquidación final de los contratos.

Con el aplicativo Orfeo, se realiza a nivel nacional el proceso de administración documental, todas las cuentas de contratistas deben ser radicadas por Orfeo y entregadas por el Grupo de Correspondencia al Grupo Central de Cuentas por Pagar, si hay errores en las cuentas, se devuelven por el mismo aplicativo y las correcciones deben venir con otro radicado; se distribuyen los radicados en las personas que revisan, luego se liquida, se registra en SIIF y salen para pagaduría, se descargan del sistema con la cuenta por pagar y obligación que se genera en SIIF.

En el proceso de pagos de servicios públicos se reciben de correspondencia las facturas, se liquida, se registra en Siif y se hace la transferencia y se descarga en el aplicativo con el número de registro de caja menor para Territoriales e Inspecciones y para planta central con cuenta por pagar y obligación SIIF.

Los pagos de nómina, sentencias, viáticos, Chatarrización; se reciben del Grupo de Administración de Personal y del Grupo de Presupuesto; el control que se tiene para estos documentos que no están radicados en Orfeo, es el registro en la base de datos de Control Cuentas por Pagar.

En el Ministerio de Transporte los procesos de pagos que se realizan en el Grupo de Cuentas por Pagar, son de apoyo al cumplimiento del objetivo central del Ministerio que es el de elaborar políticas de transporte e infraestructura en todos los modos de transporte a nivel nacional.

9.2 ANALISIS DE LA SITUACION ACTUAL DEL GRUPO CUENTAS POR PAGAR EN SEGURIDAD INFORMÁTICA

Para identificar la situación actual del grupo de Cuentas por Pagar en seguridad informática, se hace un análisis de los criterios de políticas de seguridad existentes en:

- Ministerio de Tecnologías e Información
- Ministerio de Transporte
- Normas ISO
- CONPES

9.2.1 Análisis del contenido de política de seguridad del Mintic

El Ministerio de Tecnologías de la Información, brinda a través de su página web y como estrategia de gobierno en línea un formato para usar en el diseño de las políticas de seguridad de la información, en entidades del estado.

El modelo está dado, de tal manera que solo se da el nombre de la entidad, en las partes generales, debido a que es inherente a todas las entidades del estado el

objetivo de establecer políticas de seguridad; como son minimizar riesgo, cumplir con las funciones administrativas y de seguridad de la información, apoyo a los adelantos tecnológicos, protección de los activos informáticos, fortalecer la cultura de seguridad, seguimiento, mejoras y socialización de las políticas.

Presenta principios de seguridad de la información, que deben hacer parte de las políticas de seguridad de la información, como son:

- Responsabilidad de la seguridad de la información de los funcionarios, contratistas y usuarios externos.
- Protección de la información del frente al mal uso de accesos, amenazas e instalaciones.
- Control de procesos de seguridad de los recursos tecnológicos, de red.
- Garantizar la seguridad, en todos los ciclos del sistema de información.
- Disponibilidad, continuidad y cumplimiento de los procesos.

El formato establece el alcance, la aplicabilidad, nivel de cumplimiento, responsabilidades.

En este modelo están las fases que se deben tener en cuenta para la implementación de las políticas de seguridad de la información, así:

- Fase de desarrollo: Justificación, alcance, roles y responsabilidades, revisión y aprobación de la política.
- Fase de cumplimiento: la política debe estar relacionada con los controles establecidos.
- Fase de comunicación: Socialización de las políticas, con el fin de darse a conocer a funcionarios, contratistas y usuarios, para poder realizar ajustes; según las observaciones que se den.
- Monitoreo: Seguimiento a las políticas con el fin de saber si han cumplido o no los objetivos.
- Mantenimiento: se asegura que las políticas se han ajustado y se le han realizado las actualizaciones necesarias.
- Retiro: se elimina la política, cuando ya no es necesaria en la entidad.

Las políticas de seguridad de información deben tener bien definido:

- Que es lo que se desea hacer
- Que regula
- Que deben hacer los usuarios
- A quien va dirigida
- Quienes deben cumplirla
- Responsable o responsables de las políticas
- Pasos para hacer ajustes
- Consecuencias de incumplimiento
- Fecha de vigencia de la política

Se recomienda definir un comité directivo de seguridad de la información; identificar y dar normas de uso, administración y responsabilidades de los activos informáticos; controles necesarios para el acceso con usuario y contraseñas; trazabilidad; auditoria; privacidad; confidencialidad; integridad; disponibilidad; registro; gestión de incidentes; capacitación; sensibilización y socialización. (Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia (Mintic))

Los formatos de políticas de seguridad de la información, que nos presenta el Mintic; esta dado de forma general, para ser adoptado por cualquier entidad del estado y ajustado a cada entidad en particular, según sus funciones, su estructura y sus activos informáticos.

Es un modelo, de gran ayuda para aplicar a las políticas que se van a diseñar e implementar en el grupo de Cuentas por Pagar del Ministerio de Transporte.

Este modelo presentado por el Mintic, da un énfasis especial a la responsabilidad y la aplicación de controles en la implementación de políticas de seguridad.

9.2.2 Análisis del contenido de política de seguridad del ministerio de transporte

La política de seguridad del Ministerio de Transporte, del año 2008; tomo como activos informáticos:
Información: todos los datos que se generan en el Ministerio y la clasificación respectiva como confidencial, privada y pública.

Equipos: son la red, estaciones, servidores y recursos informáticos del Mintransporte. Los clasifica en sistemas críticos y sistemas esenciales. Acá hace énfasis en los procesos que se realizan en cuanto a instalación, mantenimiento, reubicación, políticas de uso, software, acceso, licencias, hacking y antivirus de los equipos de cómputo.

Control de acceso: En este capítulo se toma en cuenta las gestiones que se deben realizar con el área de informática para:

- Autorizaciones de acceso al hardware, a la red y servidores
- Acceso a áreas críticas, como centro de datos, de cableado, tableros electrónicos, cuartos de UPS y cuartos de vigilancia.
- Control de acceso a los PC, cada equipo en el Ministerio tiene un responsable al cual el área de Informática le dará un usuario y la opción de crear su contraseña, son los responsables directos del uso de equipo asignado, el área de Informática tendrá control de administrador para verificaciones y control de uso de todos los computadores de la entidad
- Control de acceso a la red, el área de informática proporcionará los permisos de ingreso a todos los recursos de red, pero también asumirá los controles de uso de la red, existen para esto restricciones a ciertas páginas de hacking o que no tienen que ver con los objetivos que se deben cumplir en el Ministerio
- Control de acceso remoto, el grupo de informática dará los permisos para el ingreso a la red de forma remota, con las restricciones necesarias para que el uso remoto sea solo para cumplir con las funciones del Ministerio, este acceso tiene protocolo SSH, RDP, VNC
- Acceso a los sistemas administrativos, solo para usuarios con perfil administrativo, y para el ingreso a ciertas bases de datos, aplicativos que deban tener uso restringido por manejar información crítica.
- Niveles de acceso, Los funcionarios del Ministerio de Transporte son empleados públicos que deben acogerse a las reglas, disposiciones y políticas que se impartan, y una de las políticas y reglas que se deben cumplir son las que tengan que ver con la seguridad de la información, es aquí donde la oficina de informática, hace seguimiento a que cada funcionario cumpla con las directrices de seguridad impartidas.
- Acceso privilegiado: Operador, son las cuentas que tiene acceso restringido como son las de administradores, directivos de alto nivel, usuarios que tengan a cargo las copias de seguridad y acceso legal. Estos privilegios deben tener normas especiales de seguridad como son: cambio de claves cada mes, contraseñas con un alto nivel de complejidad, responsabilidad en el uso de contraseñas,

- Acceso privilegiado: Administrador, las cuentas de administrador, deben manejarse con responsabilidad, actitud, ética, buen comportamiento, hacer cumplir los derechos, atender las emergencias, velar por que se usen solo los dispositivos autorizados, seguir las conexiones de los equipos de cómputo, que se sigan los protocolos autorizados, que solo sean instalados servidores www autorizados; deben cumplir y hacer cumplir a todos los usuarios de PC y red las políticas de seguridad de la información.

Recursos de la red: El uso de red debe ser responsable y únicamente con el propósito de cumplir con los procesos establecidos en el Ministerio y el área de informática debe hacer seguimiento, actualización y control de los recursos de red. La información de red debe ser manejada por cada funcionario con responsabilidad, almacenando solo información de la entidad y en caso de tener información personal, se debe describir para que dicha información no haga parte de las copias de seguridad, no se debe almacenar en los equipos asignados música, videos, imágenes que no tengan nada que ver con las funciones asignadas.

No están autorizados servicios a la red; el sitio oficial web del Ministerio solamente es www.mintransporte.gov.co; cada área del ministerio debe mantener actualizada la información que se publique.

El área de informático es responsable del cumplimiento de las políticas de seguridad de la información, buen manejo de los recursos de red e informáticos, y buen uso del correo electrónico institucional.

Ambiente físico: hace parte del ambiente físico las instalaciones y acá se deben tener sistemas de detección y aviso de incendios, pararrayos, aplicación de cada área de normas mínimas de seguridad, como son conexión de equipos solo a la red eléctrica regulada, no se pueden consumir bebidas ni alimentos en los sitios de trabajo, no se permite el uso de fuego, acceso solo de personal autorizado a las áreas restringidas, uso de puerto a tierra y conocimiento de todos los funcionarios de los planes de evacuación existentes.

Software: El área de informática debe cerciorarse del no uso de software no licenciado en la red del Ministerio, se debe respetar la propiedad de autor del software libre, solo se debe adquirir software de sitos oficiales y seguros, solo el área de Informática podrá instalar, actualizar, desarrollar, supervisar y revisar el software que se instale en cada computador, cuando fuera el caso y con el objetivo de cumplir con las funciones asignadas; por ejemplo en la Subdirección

Administrativa se usa el aplicativo SIIF - y el área de Informática debe tener todo el control de su manejo.

Nombres de usuario y contraseñas: El área de Informática, es la encargada de proporcionar a cada funcionario del Ministerio un nombre de usuario y la habilitación de contraseñas; cuando el funcionario sea trasladado, salga de la entidad definitivamente o a vacaciones, el jefe inmediato debe reportar al grupo de Informática la novedad para que se cancelen o se inhabiliten los usuarios, según la situación, solo podrán tener usuarios los funcionarios o contratistas vinculados legalmente a la entidad, los permisos estarán de acuerdo con las funciones que cada funcionario tenga, hay límite de intento para acceso a la red, las contraseñas deben tener un buen nivel de complejidad y se deben cambiar con cierta periodicidad.

Las políticas de seguridad del Ministerio hacen énfasis en:

Respaldo y continuidad del negocio: se debe hacer seguimiento y control, para que se mantengan las normas básicas de seguridad, en los sistemas de cómputo, como son las detecciones y eliminación de fuego, unidades suplementarias de energía, filtros eléctricos, supresores de picos de energía, eliminadores de corriente estática, puntos de computo con la debida distancia, backup en sitios muy seguros, tener planes de contingencia por daños de equipos y de software, mantenimiento preventivo y correctivo a todos los equipos computacionales.

Políticas de respaldo: Se debe establecer la información objeto a ser respaldada y quien es el responsable, esta responsabilidad estará en manos de los usuarios con perfil administrador, la información que sea objeto de respaldo, debe estar guardada en dos sitios diferentes y una vez no tenga utilidad debe eliminarse.

Usos prohibidos: En el Ministerio de Transporte, está prohibido el uso de recursos informáticos con fines comerciales o personales; uso inadecuado de estos recursos como pornografía, ofensa, desacreditación a otros, propagandas, cadenas o actividades lucrativas, instalación de hardware o software no autorizado por el área de Informática; acceso sin autorización a la red institucional, usar usuarios y contraseñas diferentes a los asignados a cada persona; hackear información para modificar, borrar o copiar; uso del correo electrónico institucional, con fines diferentes para lo que fue creado; uso de software malicioso o dañino; no se puede usar la red para actividades diferentes a las laborales.

Disposiciones generales: El personal que labora en el grupo de Informática, por manejar información sensible; deberá cumplir con sus funciones acogiéndose a las normas de ética profesional, normas y procedimientos establecidos; los equipos portátiles de computación deben llevarse a la mano; los equipos portátiles deben tener un buen nivel de encriptación; todos los quipos de computo deben tener su respectivo registro de inventario y cada usuario debe manejarlos de forma segura cumpliendo con las disposiciones de seguridad dadas por el área de Informática.

Sanciones: Las políticas de seguridad de la información deben cumplirse por cada uno de los funcionarios y contratistas del Ministerio; quien haga caso omiso de estas políticas puede verse inmerso en investigación administrativa la cual cuenta con una sanción correspondiente a la acción o actividad incorrecta.

Notas finales: Las políticas de seguridad de la información deben ser actualizadas periódicamente y debe socializarse con todos los funcionarios del Ministerio a nivel nacional. (Ministerio de Transporte, 2008)

Estas políticas dan una importancia especial a los ajustes, mantenimiento y las responsabilidades puntuales en la entidad de las políticas de seguridad de la información.

A pesar de tener dentro de sus parámetros el realizar mantenimiento, ajuste y actualización periódica a las políticas de seguridad; la última versión y actualización fue en el año 2008; después de casi diez años, la tecnología, los recursos de software y hardware han evolucionado y avanzado considerablemente; los activos informáticos ya no son los mismos y los controles deben estar según los últimos avances tecnológicos.

Estas políticas fuera de llevar mucho tiempo sin actualizar, están hechas de forma muy general y no tienen la socialización necesaria, para que sirva de ayuda y control de seguridad de la información.

9.2.3 Análisis del Contenido del Documento de Normas ISO

La norma ISO 27001, nos servirá de base para la construcción de las políticas de seguridad, básicamente da las pautas para implementar hacer seguimiento, revisar y mejorar un sistema de gestión de la seguridad de la información.

La norma se centra en los procesos, adoptando el modelo de:

- **Planear**: se establecen políticas, objetivos, procesos y procedimientos de seguridad; identificar riesgos y aplicar controles de seguridad de la información.
- **Hacer**: Se implementan las políticas, controles, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información
- **Verificar**: se realiza seguimiento y evaluación a las políticas, controles, procesos y procedimientos del SGSI.
- **Actuar**: Con el informe de la verificación, se implementan los controles preventivos y correctivos, para tener un buen SGSI.

La norma ISO 27001, está dada para guiar en el diseño e implementación de SGSY, tanto a entidades públicas como privadas. Especifica el desarrollo de:

- Sistema de Gestión de la Seguridad de la Información: dando las pautas para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI, definiendo alcances, limites, políticas y hace énfasis especial en el tratamiento de los riesgos para poder aplicar los controles necesarios y suficientes a los procesos de la organización en materia de seguridad informática.
- Sobre la documentación que debe incluir el SGSI, especifica la necesidad de tener objetivos, políticas, alcances, controles, metodología, valoración y tratamiento de riesgos y aplicabilidad; debidamente documentado y soportado.
- Establece las responsabilidades de los directivos, en el compromiso, provisión de recursos y competencias de los funcionarios; en todas las etapas de implementación, desarrollo y puesta en marcha del SGSI.
- Las organizaciones deben realizar auditorías internas con el fin de verificar que se cumplan los objetivos del sistema.
- Con las auditorias, la dirección debe revisar si se están o no cumpliendo los objetivos, si hay que hacer mejoras, correcciones o ajustes y hacer el seguimiento a las acciones preventivas y correctiva que se establezcan

La OCDE (Organización para la Cooperación y el Desarrollo Económico), presenta unas directrices, que de la mano con el proceso de PHVA, servirá de apoyo para los SGSI y políticas que se establezcan en las organizaciones, así: Toma de conciencia (hacer); responsabilidad (hacer); respuesta (verificar); valoración de riesgos (planear); diseño e implementación de la seguridad (planificar); gestión de

la seguridad (planificar, hacer, verificar y actuar); reevaluación (actuar). (NTC-ISO/IEC 27001, 2013).

La norma ISO-27001, nos da especialmente herramientas para una vez identificados los activos informáticos y las posibles amenazas; establecer los objetivos de control y controles a implementar en el SGSI.

Es importante conocer todas las directrices dadas por la norma ISO 27001, sobre SGSI, que nos ayudaran a diseñar e implementar correctamente las políticas de seguridad en el Grupo de Central de Cuentas por Pagar.

9.2.4 Análisis del contenido del documento CONPES 3854

El documento CONPES 3854, establece la Política Nacional de la Seguridad Digital, centrándose más en el análisis de riesgos que en el control de amenazas.

Este documento tiene un estudio del crecimiento vertiginoso que han tenido las Tecnologías de la información en los últimos años, uso de la banda ancha, uso de internet, uso de redes sociales y uso de los correos electrónicos; dando un gran avance digital en el país y por ende también se han incrementado los ataques a la seguridad de la información.

Para ampliar las medidas de seguridad de la información se creó al documento CONPES 3854, que es una política nacional de seguridad de la información digital; complementó de políticas anteriores que solo centraban su atención en contrarrestar amenazas; este nuevo documento va más allá y sus objetivos son:

- Seguridad digital nacional centrada en los riesgos informáticos
- Gestionar el riesgo de seguridad digital en todas las actividades.
- Siguiendo el enfoque en los riesgos de seguridad, fortalecer y dar confianza a los individuos y el estado en el uso de tecnologías de información.
- Tener estrategias de cooperación nacional e internacional para el manejo seguro de la información digital en el país.

Las políticas de seguridad nacional digital, abarca todas las entidades del estado, dándole a las entidades de orden nacional y sus directivos responsabilidades

claras y precisas en la implementación de SGSI; previo análisis administrativo, económico y legal.

El objetivo de este documento al centrar su estudio e implementación de políticas en el riesgo informático; es dar confianza y seguridad a todos los usuarios de las plataformas digitales; y esto la hace fortaleciendo las entidades del estado encargadas de la seguridad informática, creando el centro criptográfico nacional, centro de excelencia de seguridad digital, centro de investigación de crímenes económicos y financieros, centros de comunicaciones, comando y control digital, laboratorio de informática forense, centro de investigación de seguridad digital. (CONPES & DNP, 2016)

Una de las partes más importantes de este documento, es la adecuación jurídica que da las pautas para poder castigar a quienes cometen delitos cibernéticos o cibercrímenes.

Este documento es de carácter oficial, para entidades del estado y nos brindan mejores prácticas que se deben tomar para asegurar la información digital nacional.

Para diseñar e implementar políticas de seguridad en el grupo de cuentas por pagar del Ministerio de Transporte; es muy importante y de mucha ayuda, tener en cuenta el análisis realizado a las políticas de seguridad de la información del M.T., modelo y plantillas establecidas por el Mintic, las normas ISO en especial la 27001 y el documento CONPES 3854 de políticas nacionales digitales. De cada una, podremos sacar información que podremos adaptar a las políticas de seguridad de la información, con el fin de hacerla más completa y más segura.

9.3 ANALISIS DE CRITERIOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL, AL ESTUDIO DE CASO DEL GRUPO DE CUENTAS POR PAGAR

Según el análisis realizado, a las políticas ya creadas por el Ministerio de Transporte, el CONPES, el Ministerio de Tecnologías de la Información, las normas ISO y la caracterización de los procesos que se realizan en el Grupo de Cuentas por Pagar, se evidencia que la seguridad de la información digital en el grupo de cuentas por pagar es muy vulnerable, de fácil acceso a la información

digital de los pagos que deben realizarse, no solo por parte de funcionarios sino también por parte de los contratistas y proveedores.

Siempre la información de pagos, en cualquier entidad, debe tener un grado de seguridad avanzado, no puede ser de fácil acceso ni debe estar desprotegido, porque los pagos son una parte importante de la contabilidad y el presupuesto de la entidad.

Vulnerabilidades y amenazas

Con el estudio realizado a los procesos de manejo de las bases de datos del Grupo Cuentas por Pagar y con ayuda de la encuesta y sus conclusiones; se evidencio que la seguridad informática, en estas bases de datos está comprometida en un alto grado; por perdida de información, dobles registros, registros incompletos, anulación de registros, pérdidas de tiempo, reconstrucción de bases de datos por perdidas de información, daños de equipos, bloqueo de las bases de datos por mal manejo, software muy antiguo e inservible.

Base de datos control cuentas por pagar:

- El acceso a las bases de datos de control de cuentas por pagar solo cuenta con un filtro de seguridad, que es el mismo que se tiene para el ingreso al equipo, contraseña que no tiene ningún tipo de restricción, no tiene que involucrar caracteres especiales y en la mayoría de equipos la clave de acceso es el mes y el año en el que se está.
- Esta base de datos controla todos los pagos que se hacen en el Ministerio, para evitar que se doblen los pagos, para informar del estado de un pago a contratistas, funcionarios, proveedores, usuarios que chatarrizan los camiones y ex funcionarios, sirve para realizar informes de pagos a los entes de control sobre los seguimientos de gestión de la oficina de planeación y de control interno.
- Por la importancia que tiene esta base de datos, debería tener una política de uso más restringido, con cifrado especial.

Base de datos servicios públicos:

- Con esta base de datos se registra y controlan los pagos realizados por cada servicio público en cada dirección territorial, inspección fluvial y planta central; evitando incurrir en pagos dobles o extemporáneos; sirve también de base para conciliación bancaria, para informes a entes de control externos como la contraloría e internos como planeación y control interno.
- Esta base de datos no tiene la seguridad que debiera tener para el tipo de información que maneja, con el ingreso al PC ya se tiene acceso a todas las aplicaciones, incluyendo la base de datos de servicios públicos, con una clave de acceso de mínima dificultad.

Base de datos relación de pagos:

- La base de datos de relación de pagos, por ser un aplicativo, obsoleto por su poca capacidad de almacenamiento y baja funcionalidad, se debe reestructurar su funcionamiento y seguridad, pues no cuenta con un cifrado especial o de alta dificultad.

Aplicativo Orfeo:

- El aplicativo Orfeo, es un software que se usa no solo en el grupo de central de cuentas por pagar sino en todo el Ministerio, está diseñado con unas mínimas medidas de seguridad, característica que afecta ampliamente su uso debido a que esta herramienta es de gran utilidad y de trascendencia para el objetivo del Ministerio, siendo los documentos el activo más importante de la gestión en la Entidad.

Es importante la creación de políticas de seguridad de la información en el grupo Central de Cuentas por Pagar, por manejarse información de cuentas, presupuesto y pagos; para que la misión del Ministerio pueda cumplirse.

Más allá de crear controles de seguridad se debe concientizar a cada usuario de las bases de datos del Grupo, en responsabilizarse de su uso, aplicando y manteniendo controles efectivos de seguridad de la información.

10. DISEÑO ESTRUCTURA DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA PARA EL GRUPO CUENTAS POR PAGAR

Con la caracterización de los procesos del Grupo Cuentas por Pagar, los análisis de políticas existentes y viendo las vulnerabilidades que tiene la información en estos procesos, se implementaran las políticas de seguridad de la información, con el siguiente diseño estructural:

1. Desarrollo de Políticas de Seguridad Informática para el Grupo Cuentas por Pagar.

1.1 Justificación

1.2 Alcance

1.3 Roles y responsabilidades

2. Gestión de activos

3. Control de acceso

4. No repudio

5. Privacidad y confidencialidad

6. Integridad

7. Disponibilidad del servicio e información

8. Registro y auditoria

9. Gestión de incidentes de seguridad de la información

10. Resultados y discusión

11. Divulgación de políticas de seguridad

12. Revisión de la política

13. Aprobación de la política

14. Cumplimiento

15. Monitoreo
16. Mantenimiento
17. Recomendaciones
18. Conclusiones
19. Retiro

11. DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL GRUPO CUENTAS POR PAGAR.

POLITICAS DE SEGURIDAD INFORMÁTICA PARA EL GRUPO CUENTAS POR PAGAR

El Grupo Cuentas por Pagar del Ministerio de Transporte, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de política de seguridad informática, en los procedimientos establecidos, buscando cumplimiento y seguridad.

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, el Grupo Cuentas por Pagar del Ministerio de Transporte, busca proteger la información que procesa, implementando buenas prácticas de seguridad.

Justificación

El objetivo de implementar política de seguridad de información, en el grupo de trabajo Cuentas por Pagar del Ministerio de Transporte, es proporcionar a los funcionarios de este grupo que manejan para el desarrollo de su trabajo aplicaciones informáticas; recursos y pautas para un manejo seguro de la información; para prevenir los riesgos que se presentan en la manipulación y manejo.

Al tener un adecuado manejo de la seguridad y blindaje de la información digital que administra el grupo de cuentas por pagar, como son las relaciones de pagos, la administración documental, pagos de servicios públicos y registro control y seguimiento de las cuentas por pagar; redundara en información concreta y veraz de todos los pagos realizados en el Ministerio de Transporte no solo en planta central sino en las Direcciones Territoriales e Inspecciones Fluviales.

Una vez diseñadas las políticas de seguridad, estas deberán ser aplicadas, por medio de la Coordinación del Grupo de Cuentas por Pagar, en cada una de las aplicaciones digitales del Grupo; beneficiándose no solo los funcionarios del Grupo sino cada una de las áreas a nivel central y nacional.

Estas políticas deben ser socializadas, para concientizar a los usuarios, sobre la importancia de asumir prácticas seguras en el manejo de la información.

Alcance

La implementación de políticas de seguridad de la información, aplicara a los funcionarios del Grupo de Cuentas por Pagar del Ministerio de Transporte, que, para desarrollar los procedimientos asignados, hacen uso de recursos informáticos, como:

- Aplicación sistema de administración documental
- Base de datos DBASE
- Bases de datos en Excel

Los funcionarios del Grupo de Cuentas por Pagar, deberán aplicar y cumplir esta política.

Roles y responsabilidades

La implementación de la política de seguridad de la información en el grupo de cuentas por pagar, es responsabilidad del profesional universitario de apoyo al Coordinador del Grupo.

La aplicación de la política, deberá ser responsabilidad de cada uno de los funcionarios del Grupo Cuentas por Pagar.

El seguimiento a las políticas de seguridad de la información en el grupo de cuentas por pagar, estará a cargo del profesional universitario que hace la implementación.

El Coordinador del Grupo de Cuentas por Pagar, autorizó el desarrollo de la política por parte de la estudiante de la especialización en seguridad informática, y autorizo su implementación.

Gestión de activos

Los activos que se manejan a diario en el grupo de cuentas por pagar, son:

Información

Es el activo más importante del Ministerio de Transporte y por ende del grupo cuentas por pagar y se debe velar por su integridad, confidencialidad, disponibilidad, adaptabilidad y seguridad.

Según la norma ISO/IEC 27001:2013, clasificaremos las políticas para la seguridad de la información, así:

Tabla 3. Políticas para la seguridad de la información

NUM.	NOMBRE	JUSTIFICACIÓN
A.5.1.1	POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	La información que se usa en el cumplimiento de las funciones, del grupo cuentas por pagar, debe tener la debida autorización y perfiles de acceso.
		La información que se maneja en el grupo cuentas por pagar, es propiedad del Ministerio y debe ser manipulada de forma responsable en el cumplimiento de las funciones; no debe ser modificada o destruida sin previa autorización; so pena de las sanciones disciplinarias correspondientes.
		El grupo cuentas por pagar en cabeza del Coordinador, es responsable de la administración segura de la información, tanto en los dispositivos de hardware, como en el software; con la debida asesoría y mantenimiento del Grupo de Informática.
		El Grupo de Informática, tiene a su cargo, establecer medidas preventivas y correctivas para asegurar la información de todas las dependencias del Ministerio de Transporte.
		La información que se maneja en el Grupo Cuentas por pagar se puede clasificar como de soporte para operaciones básicas del Ministerio, es información privada solo disponible para entes de control, responsables del proceso de pago y beneficiarios del pago.
Fuente: ISO/IEC 27001:2013 - El autor		

Equipos

El Ministerio de Transporte cuenta con una red 100baseT con topología estrella, a través de la cual se interconecta con los computadores personales, internet y aplicaciones.

En el Grupo Cuentas por pagar, cada funcionario tiene asignado un computador personal, con acceso a internet y cada uno es responsable tanto del buen uso de la maquina como del software que se use.

El mantenimiento preventivo y correctivo de los equipos es responsabilidad del Grupo de Informática, así como la verificación de la seguridad física y acondicionamientos que deban realizarse.

En cada computador asignado a los funcionarios del Grupo de Cuentas por Pagar, está instalado el software libre de administración documental Orfeo, la base de datos de Excel de control cuentas por pagar y se tienen los permisos y certificaciones necesarias para el acceso en línea al sistema financiero de la nación (SIIF). En un computador esta la base de datos Dbase para el manejo de las relaciones de pagos y en otro la base de datos Excel de servicios públicos.

Políticas de uso de computador personal y del software instalado.

Tabla 4. Políticas de uso de computador personal y del software instalado

NUM.	NOMBRE	JUSTIFICACIÓN
A.12.5	CONTROL DE SOFTWARE OPERACIONAL	El computador y el software instalado, es responsabilidad del funcionario al que le fue asignado.
		Cada funcionario debe tener la inducción necesaria en el manejo del computador y el software, asignado.
		Los pc y el software solo deben ser utilizados para labores asignadas.
		Solicitud de configuraciones, mantenimiento preventivo y correctivo; solo al personal autorizado por el Grupo de Informática.
		Cada funcionario es responsable de la seguridad del hardware y software asignado.
		No se puede instalar software diferente al autorizado e instalado por el Grupo de Informática.

Tabla 4. (Continuación)

A.12.5	CONTROL DE SOFTWARE OPERACIONAL	Solo el Grupo de Informática tiene la autorización para acceder e inspeccionar los equipos de cómputo personales y o para realizar mantenimientos, configuraciones o investigación a violaciones de la información.
		No se debe usar el computador asignado para instalar o practicar técnicas de hacking.
		Cada funcionario debe estar pendiente de que el antivirus instalado por el Grupo de Informática, este actualizado y funcionando. En caso de detectar alguna anomalía al respecto se debe informar al grupo de informática para que se apliquen los controles necesarios.
Fuente: ISO/IEC 27001:2013 - El autor		

Control de acceso

El Grupo de Informática, habilita las cuentas de usuarios a cada funcionario y contratista, para el ingreso al computador asignado. No se permite el uso de usuario anónimo.

Cada funcionario es responsable de su usuario y clave de acceso, debe ser intransferible a otros usuarios o equipos.

Controles de acceso al hardware y software asignado

La información que se maneja en el Grupo de Cuentas por Pagar, debe considerarse como privilegiada, porque es información de los pagos que el Ministerio debe realizar a nivel nacional a funcionarios, contratistas y proveedores. Pagos que son la base para que se cumplan los objetivos y la misión del Ministerio.

Por lo anterior las cuentas de usuarios de los funcionarios del Grupo Cuentas por Pagar deben estar protegidas.

Tabla 5. Políticas de acceso

NUM.	NOMBRE	JUSTIFICACIÓN
A.9.4.3	SISTEMA DE GESTION DE CONTRASEÑAS	Cada funcionario es responsable de su usuario y contraseña
		El grupo de informática está autorizado para ingreso a los equipos personales, con fines de auditoría, seguimiento, revisión o investigación, ingresando con perfil de administrador.
		Los computadores personales, solo pueden ser usados por el funcionario asignado y responsable.
		El uso inadecuado y el acceso de un tercero a un equipo personal; solo es responsabilidad del funcionario al que se le asignó el equipo y es el que deberá asumir las consecuencias.
		El Grupo de Informática, puede desconectar el equipo que esté en riesgo de funcionamiento.
		La contraseña debe ser cambiada por lo menos una vez cada 30 días.
		La contraseña debe tener un alto grado de complejidad
		La contraseña debe cambiarse, cuando se sospeche que alguien más la ha usado o la ha identificado
		La contraseña es personal e intransferible
		La información que se maneja en el grupo cuentas por pagar solo debe ser conocida por el funcionario, contratista o proveedor beneficiario del pago.
		Si por alguna circunstancia se transfiere la clave a un compañero, el buen o mal uso de esta, será responsabilidad del dueño de la cuenta.
		Uso de cifrado especial, para el acceso a la base de datos de control cuentas por pagar
		Uso de cifrado especial, para el acceso a la base de datos de servicios públicos.
		Uso de cifrado especial para el acceso a la base de datos de relación de pagos.
		Acceso responsable y ético al hardware y software asignado.
Fuente: ISO/IEC 27001:2013 - El autor		

No repudio

Para que los funcionarios del Grupo de Cuentas por Pagar, eviten cometer acciones indebidas en el cumplimiento de sus funciones.

Tabla 6. Políticas de no repudio

NUM.	NOMBRE	JUSTIFICACIÓN
A.5.1.1	POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Realizar seguimiento a la información que se suministra a terceros.
		Establecer auditorias continuas por parte del coordinador del Grupo de Cuentas por Pagar, para tener informes de las acciones indebidas y el responsable.
Fuente: ISO/IEC 27001:2013 - El autor		

Privacidad y confidencialidad

La información que se manipula en el Grupo de Cuentas por Pagar; debe ser procesada con seguridad para brindarle al usuario (funcionario, contratista o proveedor), la privacidad y confidencialidad de sus datos que son personales e intransferibles; los usuarios entregan sus datos financieros y personales al grupo en los formatos y actas establecidos y saben que solo pueden ser usados para su trámite de pago y los funcionarios saben que solo los pueden usar para tramitar el pago correspondiente.

Tabla 7. Políticas de privacidad y confidencialidad de la información

NUM.	NOMBRE	JUSTIFICACIÓN
A.5.1.1	POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Realizar seguimiento a la información que se suministra a terceros.
		Solo se podrá dar información de las cuentas por pagar al directamente responsable.
		La información que se tramita en el Grupo de Cuentas por pagar, debe cumplir con la seguridad necesaria, en las bases de datos se controlan todos los pagos que el ministerio realiza a nivel nacional, es información sensible de ser adulterada o cambiada, es ´por eso que los funcionarios del grupo deben manejarla con las medidas de seguridad técnica, administrativa y humanas que sean necesarias.
		Los usuarios tienen derecho a conocer, rectificar y actualizar sus cuentas.
A.5.1.1.	POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Toda la información de cuentas debe darse solo a la persona beneficiaria del pago o al que él o ella autoricen.
		Los funcionarios o contratistas que manipulan la información en el Grupo de Cuentas por Pagar, deben firmar un compromiso de no divulgación de la información interna y externa de los beneficiarios de los pagos; estipulando el inicio y finalización del acuerdo.
Fuente: ISO/IEC 27001:2013 - El autor		

Integridad

Todos los funcionarios del Grupo de Cuentas por Pagar, deben manejar la información que procesan de forma íntegra e integral; recibiendo, entregando o transmitiendo esta información en los medios y a las personas correspondientes y autorizadas, sin modificaciones y sin alteraciones.

Los equipos de hardware y software que se utilicen deben estar protegidos, para garantizar su integridad con antivirus, vacunas, privilegios de acceso y normas establecidas para el buen uso.

La vigencia de las políticas de integridad debe estar acorde con el tipo de vinculación de los funcionarios que manipulan la información.

Disponibilidad del servicio e información

Ante un evento de seguridad de la información, el Grupo de Cuentas por Pagar, se asumirán políticas de información.

Tabla 8. Políticas de integridad de la información

NUM.	NOMBRE	JUSTIFICACIÓN
A.5.1.1	POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Tener disponibilidad de la información, con copias de las bases de datos, con la debida actualización.
		Ante interrupciones por caídas de red, fluido eléctrico o bloqueo de las aplicaciones; se deben tomar medidas como, copias permanentes de la información que se procesa; cuando se interrumpe el fluido eléctrico; el grupo de informática tiene establecido un tiempo prudencial para que se apaguen los equipos, tiempo en que es posible guardar la información que estemos procesando; si se bloquean las aplicaciones; al restablecerse, se cuenta con autoguardado y se debe tener cuidado en usar la última versión guardada automáticamente.
Fuente: ISO/IEC 27001:2013 - El autor		

Registro y auditoria

La Oficina de Control Interno, debe realizar auditorías periódicas a los procesos que se manejan en todas las áreas del Ministerio de Transporte.

Los resultados de las auditorias de control Interno, deben ser publicados y se deben tener en cuenta para evaluar los controles que se establezcan, la eficiencia de los sistemas y el cumplimiento de normas y procedimientos del Ministerio de Transporte y recomendar el seguimiento y solución a las deficiencias que se encuentren.

Las auditorias deben tener unos registros, de las copias de seguridad y el correcto funcionamiento de las bases de datos que se manejan en el Grupo de Cuentas por Pagar

Las auditorías realizadas por la Oficina de Control Interno, se realizan en cumplimiento de la norma ISO 9004:2008 NTC GP 1000:2009.

Las auditorias deben realizarse por lo menos una vez cada trimestre para poder detectar a tiempo anomalías en los procedimientos y poder dar las soluciones pertinentes.

Gestión de incidentes de seguridad de la información

Al grupo de informática se deben reportar los incidentes que se presenten en la manipulación de la información en el Grupo de Cuentas por Pagar, así:

- Bloqueo de los equipos de cómputo asignados
- Acceso denegado a las aplicaciones
- Lentitud en el proceso de las aplicaciones
- Perdida de información
- Alteraciones de la información
- Solicitudes de mantenimiento

Para realizar estos reportes, el Grupo de Informática, tiene establecido la solicitud por correo electrónico a mesa de ayuda.

Cada funcionario del Grupo de Central de Cuentas por Pagar, debe realizar el reporte en el momento en que se presente el incidente; a su vez el Grupo de Informática, recepciona el incidente y emite un correo con la fecha en que se realizara la revisión pertinente; una vez de solucione el impase, se debe firma un formato que la persona encargada de la solución trae para dar por finalizado el reporte y la solución.

Resultados y discusión

El resultado de la encuesta realizada a los funcionarios del Grupo de Cuentas por Pagar, sobre la seguridad de las bases de datos que manipulan se pudo evidenciar que hay falencias de seguridad y se deben implementar políticas de seguridad de la información.

Con la implementación de políticas de seguridad de la información en el Grupo de Cuentas por Pagar, se debe obtener niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información que se procesa en el grupo.

Divulgación política de seguridad

La implementación de esta política de seguridad de la información en el Grupo de Cuentas por Pagar, básicamente busca dar una formación a los funcionarios que manejan las bases de datos del grupo, para el cumplimiento de los procesos asignados. Formación en temas de seguridad de la información, con el fin de disminuir las vulnerabilidades, amenazas halladas tanto a nivel de recurso humano, como de controles de acceso.

La política será divulgada a cada uno de los funcionarios del Grupo de Cuentas por Pagar, por parte de la funcionaria que elabora estas políticas.

La divulgación inicialmente se hará al grupo en general, socializando las políticas de seguridad de la información y controles de acceso; posteriormente se les hará llegar por correo electrónico a cada uno de los funcionarios.
Se realizará seguimiento al cumplimiento de las políticas por parte del Coordinador del Grupo, previo compromiso de los funcionarios del grupo de su cumplimiento.

Revisión de la política

El comité evaluador de la UNAD, realizara la respectiva revisión y aprobación de la presente política, para avalar su aplicabilidad, desarrollo y sugerencias.

Aprobación de la política

Como esta política es para implementar en el Grupo de Cuentas por Pagar del Ministerio de Transporte, quien debe aprobar su implementación, publicación y socialización, es el Coordinador del Grupo quien autorizo la realización del proyecto.

Cumplimiento

El Coordinador del Grupo de Cuentas por Pagar con ayuda de la funcionaria que elabora las políticas de seguridad de la información para el grupo, realizara seguimiento para verificar el cumplimiento de las políticas relacionadas directamente con la aplicación de los controles de información y de acceso documentados.

Monitoreo

La funcionaria que implementa las políticas de seguridad de la información en el Grupo de Cuentas por Pagar, debe hacer seguimiento periódico y evaluar si han sido efectivas y si se ha dado cumplimiento a dichas políticas; si esta verificación da como resultado el no cumplimiento de dichas políticas, deberá realizar los ajustes correspondientes.

Mantenimiento

Con los resultados del monitoreo se podrán establecer los ajustes que deban realizarse con el fin de asegurar el cumplimiento, efectividad y actualización de la política de seguridad de la información. Así como el monitoreo el mantenimiento debe realizarse periódicamente.

Recomendaciones

- Aprobación de la política de seguridad de la información en el Grupo Central de Cuentas.
- Socializar las políticas de seguridad de la información en el Grupo Central de Cuentas.
- Verificar el cumplimiento de las políticas de seguridad de la información en el Grupo de Cuentas por Pagar.
- Con la asesoría del Grupo de Informática, realizar monitoreo y mantenimiento a las políticas de seguridad por lo menos dos veces al año.
- Para el manejo de documentación y archivo de la base de datos de servicios públicos, se recomienda expedir solo una copia de la cuenta, con el original de la factura, y digitalizar los documentos y hacer un archivo digital de las cuentas y facturas por cada Dirección Territorial e Inspección y un consecutivo. De esta manera se ahorra tiempo y se evita duplicidad de archivo físico y contribuimos con el plan de 0 papel.

Conclusiones

- Aunque el Ministerio de Transporte tiene implementada una política de seguridad de la información, desde el año 2008; esta política está dada a nivel general y no tiene una verificación de cumplimiento; por este motivo fue necesario implementar una política de seguridad de la información, centralizada en el Grupo de Cuentas por Pagar, para cubrir básicamente la seguridad de la información que se procesa en el grupo.
- Una política de seguridad de la información centralizada en un grupo de trabajo, garantizara el cumplimiento de reglas específicas de seguridad, que llevaran a procedimientos agiles, confiables y seguros.
- Una buena socialización de la política de seguridad de la información en el grupo de cuentas por pagar y la concientización de cada

funcionario en el cumplimiento de reglas de seguridad de la información y controles de acceso; es la mejor herramienta de seguridad que se podrá implementar.

Retiro

El retiro de la política de seguridad de la información se realizará con la debida documentación y soportes, cuando se ha cumplido con su finalidad o ya no sea necesaria en el Grupo de Cuentas por Pagar.

CONCLUSIONES

El Ministerio de Transporte, aunque desde el año 2008 implemento política de seguridad de la información, no ha realizado ni la actualización ni el seguimiento a estas políticas; por este motivo fue necesario realizar un estudio sobre los niveles de seguridad informática, a los procedimientos realizados en el Grupo de Cuentas por Pagar.

La experiencia directa en la manipulación de la información en el Grupo de Cuentas por Pagar del Ministerio de Transporte; evidencio las amenazas y riesgos que se presentan y la necesidad de implementar medidas de seguridad informática a los procedimientos concretos que se manejan en el grupo.

Para asegurar la información digital del grupo se diseña e implementan políticas de seguridad, al interior del grupo con el fin de dar cumplimiento de reglas especificas de seguridad; reglas que se pueden verificar, seguir y actualizar.

El cumplimiento de una política de seguridad de la información, al caso específico del Grupo de Cuentas por Pagar, tendrá como resultado procedimientos agiles, confiables y seguros, y pueden servir de base para que se implementen en otros procedimientos del Ministerio de Transporte.

Para la Ingeniería de Sistemas, el tema de Seguridad Informática, adquiere día a día mayor importancia, dedicación y cuidado; pues no solo tenemos amenazas físicas y humanas, sino que cada vez se están incrementando los ataques a la información y la información está cada vez más expuesta y es más vulnerable.

Para proteger nuestra información, no solo se debe tomar una medida sino que se deben implementar una seria de controles a nivel de hardware, software y sobre todo de concientizar al personal encargado del manejo de la información digital, la importancia de aplicar controles preventivos y correctivos a la información digital.

BIBLIOGRAFIA

ADVISERA.COM. "ISO 27001". {en linea}. {consultado diciembre 2017} disponible en: https://advisera.com/27001/academy/es.

ALVAREZ BASALDÚA, L. D., "Tesis Seguridad en Informatica (Auditoría de Sistemas)". {en linea} {consultado marzo 2017} disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

BANDA, O. "Dbase". {en linea}. {consultado marzo 2017} disponible en: http://www.monografias.com/trabajos11/dbase/dbase.shtml

BUENDIA, J. F. (2013). "*Seguridad Informatica"*. {en linea}. {consultado en marzo de 2017}. Disponible en: https://Downloads/Seguridad_inform_tica%20(2).pdf

BURGOS SALAZAR, J., & Campos, P. G. (s.f.). "Modelo para Seguridad de la Información en TIC". {en linea}. {consultado marzo 2017} disponible en: http://ceurws.org/Vol-488/paper13.pdf

CABRERA M., Harold Emilio - UNAD. (2013). "Modulo Informatica Forense". UNAD

CODINA, L. (Diciembre de 2001). Las Propiedades de la información digital. Sistemas de Información, 19.

CONPES, & DNP. (2016). Política Nacional de Seguridad Digital (3854). Bogotá D.C.: República de Colombia.

CONTADURIA GENERAL DE LA NACIÓN. (s.f.). "Procedimiento funcional cuando existe una unidad ejecutora". {en linea} {consultado marzo 2017} disponible en: http://www.contaduria.gov.co/wps/wcm/connect/8e9c97e2-b46b-4329-b736-b0e0527a1317/PROCEDIMIENTO+-++UNIDAD+EJECUTORA+CON+VARIAS+ECP.pdf?MOD=AJPERES&CACHEID=8e9c97e2-b46b-4329-b736-b0e0527a1317

DIRECCIÓN NACIONAL DE PLANEACIÓN. (s.f.). "SIIF NACION". {en linea}. {consultado en marzo de 2017}. disponible en: https://colaboracion.dnp.gov.co/CDT/Inversiones%20y%20finanzas%20pblicas/Sistema_Integrado_de_Informacion_financiera_SIIF.pdf.

ESCRIVÁ R., G.G., S.R.M., && Ramada, D.J. (2013). "Seguridad Informática". {En línea}. {Consultado en marzo de 2017}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&pOO=

ESTABLECIMIENTO Y GESTIÓN DEL SGSI. (s.f.). {en linea}. {consultado en marzo de 2017}. Disponible en: https://www.blogger.com/null

FURAG (s.f.). {en linea} {consultado en diciembre de 2017} disponible en: www.sirvoamipais.gov.co

ISO 12207. (s.f.). {en linea} {consultado en marzo de 2017} disponible en: https://es.scribd.com/doc/131847881/NORMA-ISO-12207-pdf

ISO 27001 / 27002. (s.f.). {en linea} {consultado en abril de 2017} disponible en: http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

LUZARDO, I. (30 de noviembre de 2010). “Conozca las amenazas informáticas más comunes”. {en linea}. {consultado en marzo de 2017}. Disponible en: http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/

MAYTA SILES, J. G., Chuquimia Salinas, M. L., Ayrton Roberto, C. C., Kevin, G., Benjamin, N., & Tapia Altamirano, A. (27 de mayo de 2011). "Monografia completa (Seguridad en redes)". {en linea}. {consultado en abril de 2017} disponible en: https://es.slideshare.net/benjamin1991/monografia-completa-seguridad-en-redes

MENDOZA, M. A. (18 de mayo de 2015). “Welivesecurity.com- CSIRT”. {en linea}. {consultado en marzo de 2017}. Disponible en: http://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

MINISTERIO DE DEFENSA. "Cartilla Sistema SIIF Nación en el Ministerio de Defensa Nacional". {en linea}. {consultado marzo 2017}. disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Sobre_el_Ministerio/Finanzas/Cartillas%20Financieras/8589_Cartilla_Sistema_SIIF.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (Mintic). (11 de 05 de 2016). "Guia 2 - Seguridad y Privacidad de la Información". {en linea}. {consultado en abril de 2017}. disponible en: www.mintic.gov.co/gestionti/615/articles-5482_G2_politica_general.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN COLOMBIA (Mintic). (s.f.). "Modelo de Seguridad y Privacidad de la Información". {en linea}. {consultado en abril de 2017}. disponible en: www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN COLOMBIA (Mintic). (s.f.). "MSPI". {en linea}. {consultado en diciembre de 2017}. disponible en: www.mintic.gov./gestionti/615/articles-5482_Instrumentos_Evaluación_MSPI.xlsx

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN COLOMBIA (Mintic). (s.f.). "Seguridad TI". {en linea}. {consultado en abril de 2017}. disponible en: www.mintic.gov./gestionti/615/w3-article-4767.html

MINISTERIO DE TRANSPORTE. (s.f.). {en linea}. {consultado en abril de 2017}. disponible en: www.mintransporte.gov.co

MINISTERIO DE TRANSPORTE, G. I. (2008). "Políticas de Seguridad Informática. Bogotá: MT".

NTC-ISO/IEC 27001. (2013). "ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Bogotá Colombia: icontec". {en linea}. {consultado en abril de 2017}. disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

ORFEO. (s.f.). {en linea}. {consulado en mayo de 2017}. disponible en: http://www.orfeolibre.org/portal/index.php/the-news/2-uncategorised/63-sgd-leermas

PVR. (s.f.). {en linea}. {consultado en mayo de 2017}. disponible en: https://dirinfra.mintransporte.gov.co/pvr2/

RAMSOMWARE. {En línea}. {Consultado en septiembre de 2017}. Disponible en: https://www.avast.com/es-es/c-ransomware

ROMERO, R. M., & Ramada, D. (2013). Seguridad Informática. Madrid: Macmillan Iberia S.A.

ROSA, I. J. (2014). “Manejo de evidencia digital”. {en linea}. {consultado en marzo de 2017}. Disponible en: http://www.infotegra.com/preview/UNAD.php?url=/bitstream/10596/2660/3/12752280.pdf

RUNT. (s.f.). {en linea} {consultado en mayo de 2017}. disponible en: http://www.runt.com.co/portel/libreria/php/02..html?dif=db5d0e705da07f69a6fc070ccd5e0dad

SÁNCHEZ VANDERKOST, E. J. (s.f.)."Panorama de la Investigación sobre Políticas de Información en America Latina". {en linea}. {consultado en mayo de 2017}. disponible en: http://www.scielo.org.co/pdf/rib/v29n1/v29n1a7.pdf

SGR. (s.f.). {en linea} {consultada en mayo de 2017}. disponible en: https://www.sgr.gov.co/.

SGSI. "Blog especializado en Sistemas de Gestión de Seguridad de la Información". {En línea}. {Consultada en septiembre de 2017}. Disponible en: http://www.pmg-ssi.com/2016/06/que-debe-incluir-en-su-politica-de-seguridad-de-la-informacion-basado-en-la-norma-iso-27001/

SISTEMA DE INFORMACIÓN. "Tipos de Información". {en línea} {Consultada en septiembre de 2017}. Disponible en: https://www.gestiopolis.com/los-tipos-de-sistemas-de-informacion-en-las-empresas/

SOLARTE, F. N. (4 de julio de 2016). "*Norma UNE-ISO/IEC 27001"*. {en linea}. {consultado en marzo de 2017}. Disponible en: http://blogsgsi.blogspot.com.co/2016/07/normal-0-21-false-false-false-es-co-x_4.html

TENDENCIAS EN SEGURIDAD INFORMATICA. "Tendencias Informáticas 2016". {En línea}. {Consultada en marzo de 2017}. Disponible en: https://info.microsoft.com/rs/157-GQE-382/images/ES-XL-CNTNT-ebook-Security-Trends-in-Cybersecurity.pdf

TARAZONA., CESAR .H.. "Amenazas informáticas y seguridad de la información". {en linea}. Consultada en marzo de 2017}. Disponible en: http://revistas.uexternado.edu.co/index.php/derpen/article/view/965

UMUS. (s.f.). {en linea}. {consultado en mayo de 2017}. disponible en: https://www.mintransporte.gov.co/Publicaciones/Ministerio/Dependencias/viceministro_de_transporte/direccion_de_transporte_y_transito/grupo_unidad_de_movilidad_urbana_sostenible_-_umus

ANEXOS

Anexo A Formato RAE

ANEXO A DOCUMENTO RAE
TIPO DE DOCUMENTO: Trabajo de grado para optar el título de ESPECIALISTA EN SEGURIDAD INFORMATICA
TITULO: DISEÑO E IMPLEMENTACIÓN POLÍTICA DE SEGURIDAD DE INFORMACIÓN, DEL GRUPO DE TRABAJO CUENTAS POR PAGAR DEL MINISTERIO DE TRANSPORTE.
AUTOR: María Elena Marín Ospina
LUGAR: Bogotá D.C.
FECHA: Noviembre 28 de 2017
PALABRAS CLAVE: política, seguridad, información, equipos informáticos, controles, acceso, responsabilidades, base de datos, SIIF.
DESCRIPCION DEL TRABAJO: El presente proyecto aplicado es un trabajo de grado para optar el título de Especialista en Seguridad Informática y tiene como objetivo diseñar e implementar política de seguridad de información, del grupo de trabajo Cuentas por Pagar del Ministerio de Transporte; realizar la respectiva socialización, seguimiento y actualizaciones necesarias.
LINEA DE INVESTIGACIÓN: Proyecto aplicado
FUENTES CONSULTADAS: Para este proyecto aplicado se consultaron, 3 políticas de seguridad, 1 tesis, 2 monografías, 9 referencias de libros en la web, 16 referencias de artículos de la web y 1 blog; todo sobre políticas de seguridad de la información y se realizó observación directa a los procesos y procedimientos del Grupo de Central de Cuentas por Pagar del Ministerio de Transporte.

CONTENIDOS: Inicialmente se hace el planteamiento del problema de seguridad de la información en el Grupo de Cuentas por Pagar del Ministerio de Transporte, se definen objetivos, justificación, marco de referencia, alcances y metodología; en la parte final se caracteriza el funcionamiento del Grupo de Cuentas por Pagar, se analizan 3 políticas de seguridad ya establecidas y la norma ISO, y se establece la situación actual de seguridad de la información en el grupo; se estructuran las políticas de seguridad y se desarrollan las políticas de seguridad de la información en el Grupo de Cuentas por Pagar del Ministerio de Transporte
METODOLOGIA: Este es un trabajo donde se usó metodología descriptiva, explicativa y de observación directa.
CONCLUSIONES: Verificando la existencia de los riesgos de seguridad de la información en el Grupo Central de Cuentas por Pagar; se proyecta la implementación de políticas de seguridad de la información, en el grupo.
Implementando las políticas de seguridad de la información en el Grupo de Cuentas por Pagar en el Ministerio de Transporte, se podrán tener a la mano las pautas y controles a seguir por cada funcionario del grupo y así evitar robos, pérdidas, destrucción o alteración de la información que se procesa en el grupo.
Una política de seguridad de la información centralizada en un grupo de trabajo, garantiza el cumplimiento de reglas específicas de seguridad, que dará como resultado procedimientos agiles, confiables y seguros.
Una buena socialización de la política de seguridad de la información en el grupo de cuentas por pagar y la concientización de cada funcionario en el cumplimiento de reglas de seguridad de la información y controles de acceso; es la mejor herramienta de seguridad que se pueda implementar en una organización.

Anexo B. Instrumento evaluación MSPI

Portada

EVALUACIÓN DE EFECTI

No.	Evaluación de Efectividad de controles	
	DOMINIO	Calificación Actual
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50
A.8	GESTIÓN DE ACTIVOS	70
A.9	CONTROL DE ACCESO	45
A.10	CRIPTOGRAFÍA	45
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	70
A.12	SEGURIDAD DE LAS OPERACIONES	70
A.13	SEGURIDAD DE LAS COMUNICACIONES	70
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60
A.15	RELACIONES CON LOS PROVEEDORES	60
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA	50
A.18	CUMPLIMIENTO	50
PROMEDIO EVALUACIÓN DE CONTROLES		**56**

Escala de evaluación

Tabla de Escala de Valoración de Controles		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Levantamiento de información

NO.	DATOS E INFORMACIÓN A RECO
	Lista de informació
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)
2	Misión
3	Análisis de contexto: La entidad debe determinar los aspectos externos e inte
4	Mapa de Procesos
5	Organigrama de la entidad, detallando el área de seguridad de la información
6	Políticas de seguridad de la información formalizada y firmada
7	Organigrama, roles y responsabilidades de seguridad de la información, asigna

Áreas involucradas

Control interno	Revisiones de seguridad de la información		
	Revisión independiente de la seguridad de la información		
	Cumplimiento con las políticas y normas de seguridad.		
	CUMPLIMIENTO		
	Auditoría Interna Plan		
	Auditoría Interna Ejecución y Subsanación de hallazgos y brechas		
Gestión humana	Selección e investigación de antecedentes		
	Términos y condiciones del empleo		
Líder de Proceso 1	**PROCESO**		
	DESCRIPCIÓN DEL PROCESO		

Pruebas administrativas

POLITICA DE SEGURIDAD DE LA INFORMACION						
AD.1	Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACION	Orientacion de la direccion para gestion de la seguridad de la informacion	A.5	Componente planificacion y madurez nivel gestionado	
AD.1.1	Responsable de SI	Documento de la politica de seguridad y privacidad de la informacion	Se debe definir un conjunto de politicas para la seguridad de la informacion aprobada por la direccion, publicada y comunicada a los empleados y a las partes externas pertinentes	A.5.1.1	Componente planificacion y madurez inicial	ID.GV-1
AD.1.2	Responsable de SI	Revision y evaluacion	Las politicas para seguridad de la informacion se deberian revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuacion y eficacia continuas.	A.5.1.2	componente planificacion	
RESPONSABILIDADES Y ORGANIZACION SEGURIDAD INFORMACION						
A2	Responsable de SI	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION	Marco de referencia para iniciar y controlar la implementacion y la operacion de la seguridad de la informacion dentro de la organizacion. Garantizar la seguridad del teletrabajo y el uso de los dispositivos moviles	A.6		
AD.2.1	Responsable de SI	Organizacion interna	Marco de referencia para iniciar y controlar la implementacion y la operacion de la seguridad de la informacion dentro de la organizacion	A.6.1	Componente planificacion y modelo de madurez gestionado	
AD.2.1.1	Responsable de SI	Roles y responsabilidades para seguridad de la informacion	Se deben definir y asignar todas las responsabilidades de la seguridad de la informacion	A.6.1.1	Componente planificacion	ID.AM-5 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1
AD.2.1.2	Responsable de SI	separacion de deberes / tareas	Los deberes y areas de responsabilidad en conflicto se deben separar para reducir las posibilidades de dar modificacion no autorizada o uso no intencional, del uso inadecuado de los activos de la organizacion.	A.6.1.2		PR.AC-4 PR.DS-5 RS.CO-5
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Una organizacion debe definir y mantener procedimientos que especifiquen cuando y por quien las autoridades deben ser contactadas (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de regulacion	A.6.1.3		RS.CO-2

Pruebas técnicas

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	ERSEGURID
CONTROL DE ACCESO						
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componentes planificación y modelo de madurez nivel gestionado**	
T.1.1	Responsable de SI	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**A.9.1**	Modelo de madurez definido	
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		PR.AC-4 PR.DS-5 PR.PT-3
T.1.2	Responsable de SI	**GESTIÓN DE ACCESO DE USUARIOS**	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**	**A.9.2**	Modelo de madurez gestionado cuantitativamente	
T.1.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		PR.AC-1

Avance PHVA

MPONEN	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	RSEGURI
PLANIFICACIÓN	P.1	Responsable	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar apobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se consideraró: 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar	
	P.2		Políticas de seguridad y	Se debe definir un	Solicite la política de	
	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	Solicite Formatos de procesos y procedimientos debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso,	
	P.4	Responsable	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la	
	P.5	Responsable	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s	
	P.6	Responsable	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	1) Solicite a la entidad la metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluacione	ID.RA-5 ID.RM-1 ID.RM-2 ID.RM-3
	P.8	Responsable	Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	1) Solicite el plan de tratamiento de riesgos y la declaración de aplicabilidad verifique que: a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Se determinaron todos los controles	ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3
	P.9	Responsable	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios,	

FUNCIÓN NIST	SUBCATEGORIA NIST	CONTROL ANEXO A ISO 27001	CARGO	REQUISITO	HOJA	CALIFICACIÓN
DETECTAR	DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-5	n/a	sponsable de	La detección de actividades anómalas se realiza oportunamente y se entiende el impacto potencial de los eventos: 1) Se establece y gestiona una linea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas. 2) Se	n/a	0
DETECTAR	DE.AE-1	n/a	sponsable de	La efectividad de las tecnologías de protección se comparte con las partes autorizadas y apropiadas.	n/a	0
IDENTIFICAR	ID.BE-2	n/a	sponsable de	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	n/a	0
IDENTIFICAR	ID.GV-4	n/a	sponsable de	en cuenta lo:	n/a	0
RESPONDER	.CO-4, RS.CO	n/a	sponsable de	Las actividades de respuesta son coordinadas con las partes interesadas tanto internas como externas, segun sea apropiado, para incluir soporte externo de entidades o agencias estatales o legales.: 1) Los planes de respuesta a incidentes estan	n/a	0
RECUPERAR	RC.CO-1, RC.CO-2, RC.CO-3	n/a	sponsable de	Las actividades de restauración son coordinadas con las partes internas y externas, como los centros de coordinación, proveedores de servicios de Internet, los dueños de los sistemas atacados, las víctimas, otros CSIRT, y proveedores.: 1) Se	n/a	0

Madurez MSPI

Madurez	R5	100	20
Administrativas	AD.1.1	0	20
PHVA	P.1	0	100
Tecnicas	T.7.1.4	0	100
		100	650
Madurez	R9	80	100
Madurez	R9	40	N/A
PHVA	P.6	0	100