PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR.

LUIS OLMEDO PATIÑO ALPALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"

ESPECIALIZACION EN SEGURIDAD INFORMATICA

SAN JUAN DE PASTO

2014

PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR.

LUIS OLMEDO PATIÑO ALPALA

Trabajo de grado para optar al título de Especialista en Seguridad informática

Asesor

ANIVAR CHAVES TORRES

Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"

ESPECIALIZACION EN SEGURIDAD INFORMATICA

SAN JUAN DE PASTO

2014

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

_____

Jurado

San Juan de Pasto, 11 de septiembre 2014

A toda mi familia,
Mis padres: Hernando y Elvira, y mis hermanos
A mi esposa María
Mis hijos: Diana Elizabeth,
Christian Mauricio y
Byron Alexander
A mi nieta Juliana
Porque todos han tomado parte
y han contribuido
en el desarrollo de este proyecto.

Luis Olmedo Patiño Alpala

AGRADECIMIENTOS

Este trabajo ha requerido de esfuerzo y mucha dedicación por parte del autor, asesor de tesis y profesores que intervinieron en el proceso, no hubiese sido posible su finalización sin la cooperación desinteresada de todas y cada una de las personas que a continuación se citarán y muchas de las cuales han sido un soporte muy fuerte en momentos de angustia y desesperación.

Primero y antes que nada, dar gracias a Dios, por estar con nosotros en cada paso que damos, por fortalecer nuestro corazón e iluminar nuestras mentes y por haber puesto en nuestro camino a aquellas personas que han sido nuestro soporte y compañía durante todo el periodo de estudio.

Agradecer hoy y siempre a nuestras familias quienes han brindado apoyo en procura de nuestro bienestar.

Al ingeniero Anívar Chaves a quien considero como uno de los mejores asesores que he tenido a lo largo de mi educación y quien me proporcionó consejos y sugerencias en el proceso y desarrollo del presente proyecto.

A la ingeniera Adriana Aguirre Coordinadora del programa de Ingeniería de Sistemas y al Magister Sixto Campaña, quien me invitó personalmente a cursar la especialización.

A los ingenieros y profesionales de la compañía donde se llevó a cabo la investigación, por su valiosa colaboración y por hacer posible el desarrollo del proyecto.

Agradecimientos a todo el cuerpo docente de la universidad e ingenieros de la Especialización en Seguridad Informática de la UNAD quienes son los formadores de profesionales y quienes contribuyen a formar un país con mejores oportunidades de desarrollo, porque en el conocimiento está el poder de una región o nación.

Luis Olmedo Patiño Alpala

CONTENIDO

Pág.

LISTA DE CUADROS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCION.

La presente investigación se llevó a cabo en una compañía prestadora de servicio público, constituida en una Sociedad Anónima con la participación de acciones del gobierno y la empresa privada, catalogada como compañía mixta por tener acciones privadas (1%) y del Estado (99%). El servicio público es comercializado con el fin de suplir necesidades básicas, bridar bienestar y confort en los hogares de los municipios, poblaciones y ciudades del departamento de Nariño y que por motivos administrativos y de comercialización se encuentra distribuida en cinco (5) zonas a saber: centro, occidente, norte, sur y pacífico; con oficinas en siete (7) seccionales, como: la Unión, La Cruz, San Pablo, Ipiales, Túquerres, Tumaco y Pasto. Los miembros de la junta directiva son representantes nombrados por el ministerio de Minas y Energía.

En atención a la Ley 1273 de 2009)[1] y Circular 052 de 2007 Superintendencia Financiera de Colombia[2], se omite el nombre y actividad económica de la compañía y que para efectos del presente proyecto para optar el título de Especialista en Seguridad Informática se le asigna el seudónimo de PROPOLSINECOR.

PROPOLSINECOR es una compañía que está creciendo en forma vertiginosa y cada vez se hace necesario la implementación de nuevos programas de desarrollo tecnológico para el control y proyección del negocio cumpliendo exigencias regulatorias y de Ley, encaminados a la reducción de pérdidas económicas y administrativas, recuperación de cartera y comercialización del servicio público, en busca del bienestar de sus trabajadores y

[1] **TÍTULO VII BIS.** De la Protección de la Información y de los datos. **CAPÍTULO I.** de los Atentados Contra la Confidencialidad, la Integridad y la Disponibilidad de los Datos y de Los Sistemas Informáticos. El presente título y los artículo que lo configuran fueron creados por virtud de la ley 1273 de 5 de enero de 2009; Ley ésta que fuera publicada en el Diario Oficial Número 47.223 de 5 de Enero de 2009 y forma parte del **CODIGO PENAL COLOMBIANO LEY 599 DE 2000.**

[2] 25 de octubre de 2007- SFC expide la CE 052, objetivo: instruir a las entidades sometidas a inspección y vigilancia sobre los requerimientos mínimos de seguridad y calidad para el manejo de la información a través de los diferentes medios y canales utilizados para la distribución de los productos y servicios que se ofrecen a los clientes y usuarios. Modificada por la circular externa 022 de 2010 y la circular externa 026 de 2011.

sus clientes, con atención oportuna a sus reclamos y fallas que se puedan presentar en la prestación del servicio, es muy importante que todos los programas informáticos u otro proyecto tecnológico se implementen con las mejores tecnologías en informática tanto en equipos de comunicación, de cómputo y software existente en el mercado, para situar a la compañía a la par del desarrollo tecnológico del país. En la implementación de estos nuevos programas o proyectos, no se puede dejar a un lado la seguridad de la información, que cambia de acuerdo a los procesos establecidos para la comercialización del servicio público y algunas políticas de seguridad informática (PSI) existentes pueden estar obsoletas y ser innecesarias en los nuevos proyectos o programas que la compañía prepara cada año para su desarrollo y eficiencia en el negocio y por lo tanto se requiere de nuevas PSI estén de acuerdo a la implementación de las nuevas tecnologías de seguridad informática y desarrollo en la prestación del servicio público.

Este proyecto se realiza con el fin de valorar los activos informáticos, analizar las vulnerabilidades, amenazas y riesgos existentes en la seguridad informática, que puedan afectar los recursos y prestigio de la compañía; para contrarrestar y mitigar los riesgos en seguridad informática, se diseña una propuesta de actualización, apropiación e implementación de Políticas claras de Seguridad de la Información, acordes al negocio y actividades de la compañía, para ser aprobadas por la alta gerencia, difundidas e implementación por PROPOLSINECOR.

En este orden de ideas, con el presente proyecto se pretende actualizar, apropiarse y establecer políticas de seguridad de la información, que protejan los activos de información, teniendo en cuenta la infraestructura y los últimos aplicativos o procesos de manejo de información implementados en la compañía, para ello se estudiará el marco teórico referente al tema, se identificarán activos de información, vulnerabilidades y amenazas en la seguridad informática, para estructurar una matriz de riesgos que permitirá determinar acciones de solución a corto, mediano y largo plazo, con el propósito de eliminar o mitigar el riesgo informático y salvaguardar activos de información que son el eje principal de toda gestión de seguridad de la información.

1. PROBLEMA DE INVESTIGACION

1.1. DESCRIPCION

PROPOLSINECOR cuenta actualmente con una infraestructura de red compleja y con diferentes medios de comunicación, para el manejo de aplicaciones del sistema operacional, comercial y financiero, para lo cual tiene implementado un "**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION**", que son unos apartes de la norma ISO NTC 27001 aplicados a los procesos de mayor relevancia; pero con políticas de seguridad informática, que no están debidamente documentadas, aprobadas y difundidas en la compañía; los usuarios del sistema informático pueden desconocer los cuidados de seguridad informática que se deben tener y por ingenuidad realizan acciones inseguras, como por ejemplo utilizar una sola clave para todo, instalar software pirata, etc; situando los activos de información en riesgo para la compañía, con los posibles daños económicos que pueden afectar el normal desarrollo de sus actividades.

1.2. FORMULACION

¿Cuáles son los riesgos de la seguridad informática en los activos de información y de negocio de PROPOLSINECOR y cómo mejorar la seguridad de los mismos?

1.3. SUBPREGUNTAS

¿Cuáles son las políticas de seguridad informática definidas y aplicadas actualmente?

¿Cuáles son las vulnerabilidades, amenazas y riesgos en la seguridad informática actuales?

¿Dadas las condiciones actuales de PROPOLSINECOR que cambios se requieren en las políticas de seguridad informática?

¿Cómo conseguir que el personal y los funcionarios se apropien, conozcan y apliquen las políticas de seguridad informática?

1.4. OBJETIVOS

1.4.1. Objetivo General.

Diseñar una propuesta de PSI normativas y procedimientos de buenas prácticas, que permitan salvaguardar los activos de información de PROPOLSINECOR.

1.4.1.1. Objetivos Específicos.

- ✓ Identificar los activos de información y de negocio en la compañía.
- ✓ Analizar las vulnerabilidades, amenazas y riesgos existentes en los sistemas de información.
- ✓ Valorar los estándares en la seguridad informática implementados en la compañía.
- ✓ Elaborar un plan de sensibilización, difusión y capacitación en políticas de seguridad informática.

1.5. JUSTIFICACION

Esta investigación permite verificar el cumplimiento de normas sobre protección de datos, privacidad, control de la información y la eficacia del "SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION" implementado por la compañía a sus sistemas más sensibles como son la Financiera y Comercial, afianzándose en apartes de la norma NTC ISO 27001[3], lo que permitirá realizar un aporte a la metodología de aseguramiento informático.

Teniendo en cuenta que la compañía ha tenido un crecimiento continuó durante los últimos años, es posible que tenga problemas para determinar quién decide qué cosas, quién es responsable de determinados activos de la información, quién debe autorizar el acceso a los sistemas de información, etc.

[3] NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de la Gestión de la Seguridad de la Información (SGSI) Requisitos. Norma Técnica Colombina. Incontec Internacional.

Al realizar un análisis de seguridad en los activos informáticos y redes o sistemas de comunicación implementados en PROPOLSINECOR, permite identificar:

- ✓ Vulnerabilidades y amenazas que existen en sus sistemas de información.
- ✓ Aplicabilidad de estándares de seguridad informática.
- ✓ Funcionalidad de las políticas de seguridad informática.
- ✓ Y eso a su vez posibilita:
  - ➢ Corregir las vulnerabilidades, amenazas y riesgos encontrados en seguridad informática.
  - ➢ Asegurar la funcionalidad y calidad de sus sistemas de información.
  - ➢ Mejorar la seguridad de sus activos de información y sistemas de comunicación.

Siguiendo este orden de ideas es de obligatorio cumplimiento tener políticas de seguridad informática actualizadas, documentadas, aprobadas e implementadas como cumplimiento regulatorio, legal y técnico; estandarizar actividades similares y responsabilidad en los diferentes lugares de trabajo; obtener las mejores prácticas seguras de trabajo en seguridad informática; identificar la filosofía de la compañía con el trabajo.

1.6. DELIMITACION

Aunque la compañía tiene sedes en diferentes ciudades del departamento, el estudio se limitara exclusivamente a una de las sedes en la ciudad capital (San Juan de Pasto), ya que los mismos procesos se aplican en todas las sedes ubicadas en otras ciudades del departamento de Nariño.

En cuanto a la limitación temática se tiene como objetivo identificar las políticas de seguridad informática de acuerdo a la norma ISO NTC IEC 27001[4], que permiten brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes, estas políticas de

[4] NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de la Gestión de la Seguridad de la Información (SGSI) Requisitos. Norma Técnica Colombina. Incontec Internacional.

seguridad informática deben salvaguardar los activos de información acorde a las vulnerabilidades y posibles amenazas de seguridad de la información identificadas en la compañía.

2. MARCO DE REFERENCIA

2.1. ANTECEDENTES

En los antecedentes se investiga los proyectos, tesis y estudios realizados con la temática de seguridad informática. A nivel nacional se tiene los siguientes estudios como: La Asociación Colombiana de Ingenieros de Sistemas (ACIS), llevo a cabo una encuesta a través de Internet del tema: **Seguridad Informática en Colombia Tendencias 2012-2013**[5], con la participaron de 162 encuestados de nuestro país, de mayor a menor de los sectores de gobierno, publico, salud, telecomunicaciones, consultoría especializada, energía e hidrocarburos, manufacturas, fuerzas armadas, construcción e ingeniería, alimentos y otros; para lo cual aplicaron un cuestionario de 39 preguntas que da a conocer como las organizaciones perciben la seguridad de la información en las Organizaciones Nacionales. Al respecto Andrés Ricardo Almanza Junco[6] en el 2013 escribe los 10 principales hallazgos del resultado de la encuesta que se describen a continuación: las organizaciones cada vez están más preocupadas por las anomalías electrónicas que asechan a internet; consideran que los profesionales de la seguridad informática deben ser certificados como una tendencia a nivel nacional; las organizaciones cada vez crean programas de seguridad informática asignado mayor presupuesto con el fin de mitigar los riesgos en las organizaciones; las instituciones educativas no hacen la suficiente difusión en los programas de seguridad informática; las organizaciones han visto a la seguridad informática con una perspectiva compleja y difícil de adoptar por el flujo de información; el presupuesto en seguridad informática lo utilizan en infraestructura con una tendencia de aumento en las

[5] http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013.

[6] Andrés Ricardo Almanza Junco, M.Sc. Ingeniero de Sistemas, universidad Católica de Colombia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia. Máster de Seguridad Informática de la Universidad Oberta de Cataluña, España. Certificación LPIC1, Linux Professional Institute. ITILv3, Auditor Interno ISO 27001:2005. Codirector de las Jornada Nacional de Seguridad Informática. Coordinador en Colombia de la Encuesta Nacional de Seguridad Informática. Coordinador de Seguridad de la Información de la Cámara de Comercio de Bogotá. www.acis.org.co/.../132-seguridad-informática-en-colombia-tendencias.

organizaciones como se muestra a nivel internacional; el 95% consideran al antivirus como una herramienta de seguridad informática; preocupación por las anomalías presentadas; los presupuestos asignados lo utilizan como primera medida en evaluar la seguridad de las plataformas informáticas; muchos no conocen los incidentes ocurridos en las compañías, lo que hace pensar que no existe atención a los incidentes y por último es una clave utilizar buenas practicas encaminadas a la construcción de modelos adecuados a que se amolden a la compañía lo que indica una madures en la seguridad informática.

Otro tema investigado por: Sandra Milena Daza Triana y Mauricio Andrés Giraldo Murillo, en la Universidad de EAN de la facultad de Ingeniería de la ciudad de Bogotá Colombia, quienes proponen el siguiente proyecto de grado titulado **Aplicación de un Sistema de Gestión de Vulnerabilidades para la Infraestructura Informática de ABC Ltda**[7]**,** en la cual plantean el siguiente problema ABC requiere un marco de trabajo que le permita la incorporación de buenas prácticas aplicadas a sus procesos y procedimientos, que garanticen una gestión adecuada a las vulnerabilidades de la infraestructura informática para contribuir en el cumplimiento de sus compromisos contractuales; y como objetivo del proyecto mencionado; para ello realizan un análisis a la infraestructura de la compañía identificando vulnerabilidades y amenazas de seguridad informática, que por cada vulnerabilidad realizan unas recomendaciones, proponiendo un plan de acción para mitigar los riesgos y protección de la infraestructura informática de la compañía .

Otros antecedentes importantes de estudios de la seguridad de la información están a nivel internacional como podemos observar en los siguientes casos:

Erik Ivan Cruz y Diana Vanessa Rodríguez del Instituto Politécnico en la ciudad de México, en noviembre de 2010 realizan la tesis de grado titulada **Modelo de Seguridad para la Medición de Vulnerabilidades y Reducción de Riesgos en Redes de Datos**[8]; para lo cual consideran que la seguridad informática en las redes de comunicación es un

[7] Biblioteca Digital Minerva.ttp://biblioteca.universia.net/html_bura/ficha/params/title/aplicacion-sistema-gestion-vulnerabilidades-infraestructura-informatica-abc-ltda/id/55867643.html
[8] http://tesis.ipn.mx/jspui/bitstream/123456789/8428/1/IF2.52.pdf.

tema muy importante de abordar, ya que un fallo puede resultar muy costoso en lo relativo a la productividad, eficiencia, pérdida de datos e información valiosa y para proteger la información de dichas organizaciones es recomendable el uso de modelos y/o prototipos que ayuden a su medición para la detección de vulnerabilidades y riesgos que pueden existir en dicha red y por tanto poder minimizar los mismos. Para lo cual proponen crear un modelo de seguridad informática conociendo los problemas de inseguridad, los ataques y amenazas a las redes empresariales conectadas o en uso a través de redes de datos e internet y dar soluciones tecnológicas, para garantizar un adecuado nivel de seguridad informática integral en la trasmisión de datos, para medir vulnerabilidades, reducir los riesgos de la redes de datos y facilitar al administrador de red conocer dichas vulnerabilidades, riesgos en donde a su vez puedan minimizarlos para la protección de la información. Para ellos se utiliza la metodología de recopilación de información que le permite la identificación de activos de la compañía a proteger, así como los factores de riesgos a los cuales se ve expuesta la red de datos de la mencionada compañía , por otra parte se deduce mediante pruebas y herramientas empleadas en la infraestructura de la red para identificar vulnerabilidades, amenazas y riesgos, que luego son analizadas y valoradas utilizando técnicas debidamente para presentar en el informe final para el administrador de la red de datos en la compañía , con el fin de implementar procedimientos de gestión de la seguridad de la información de acuerdo al modelo propuesto, que se basa en verificar, probar e intentar vulnerar aquellos agujeros de seguridad informática, que puedan estar presentes en la red de datos y que en muchas ocasiones pasan inadvertidas ante los administradores de red (CRUZ y RODRÍGUEZ 210).

(DE FREITAS 2009), propone: Conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que se encuentran en custodia por la Dirección de Servicios Telemáticos (DTS) de la Universidad Simón Bolívar ubicada en Caracas estado de Miranda Venezuela, como una continuación a un trabajo de seguridad de la información en base a los controles de la ISO 17799:2005, estudio retomado en el año 2009; el cual considera que por manejar grandes volúmenes de información, diversidad e

importancia; puede ser blanco de posibles ataques, La Universidad forma personas con habilidades que mal dirigidas pueden representar una amenaza. Una vez realizado el análisis de activos de información, ponderado los riesgos, identificado los controles concluye que: **La DST debe promover el establecimiento, implementación, operación, monitoreo, mantenimiento y mejoramiento de ISO 27001-2007 en la Universidad Simón Bolívar[9].**

También se tiene que: Jorge Colinas Ramírez de la Universidad Pontificia Comillas, propone como proyecto de fin de carrera un plan de seguridad informática, para una pequeña compañía ubicada en Madrid España, en septiembre del 2008, quien realiza un análisis de la compañía Arroyo Fuenzaldaña ubicada en Valladolid, buscando evaluar el nivel de seguridad de sus datos y proceso informáticos, para lo cual realiza un estudio del estado actual de la pequeña compañía determinando las vulnerabilidades, amenazas y el impacto que causarían sobre la compañía y adoptando las medidas necesarias para conseguir un alto nivel de seguridad informática con las recomendaciones implementadas. Como conclusión realizan un plan de mejoramiento de la seguridad informática en la pequeña compañía (RAMÍREZ 2008).

Otro estudio de seguridad informática está desarrollado por: María Gabriela Hernández Pinto quien realiza la tesis llamada: Diseño de un Plan Estratégico de Seguridad de Información en una Compañía del Sector Comercial. En el año 2006 en la Escuela Superior Politécnica Del Litoral, en Guayaquil Ecuador quien plantea *un* modelo de seguridad de la información orientado al cumplimiento de normas, procedimientos y estándares informáticos con el objetivo de crear una cultura de seguridad en la compañía, mejorando las seguridades existentes en informática requeridas para la salvaguarda de la integridad de los recursos informáticos", (HERNÁNDEZ, 2006). En base a lo anterior plantean desarrollar un procedimiento de identificación y evaluación de riesgos, determinando controles, en base a los incidentes y amenazas, elaboración de una matriz valorando el

[9] Scielo. http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=en&nrm=iso&ignore=.html

factor de riesgo, con el fin de plantear un plan de seguridad informática, teniendo en cuenta las actividades de la compañía; con el objetivo de plantear un programa modelo de estrategia se seguridad de la información, para ser implementado en cualquier compañía de actividad comercial, con el único fin de salvaguardar la información, en vista de que a través de la historia los ataques informáticos a las organizaciones comerciales son más frecuentes, causando daños irreparables; para ello propone un plan estratégico para lograr un balance optimo entre las oportunidades de tecnología de información y los requerimientos del negocio, a través de un proceso de planeación estratégica realizando recomendaciones en la implementación de la seguridad informática en base al análisis de una matriz de riesgos informáticos considerados como de mayor amenaza.

2.2. MARCO TEÓRICO CONCEPTUAL

2.2.1. Seguridad Informática.

La preocupación interna de una compañía en proteger la información, cobra cada vez más fuerza debido al creciente desarrollo tecnológico en las actividades de negocio, aplicación de regulaciones vigentes y fallas electrónicas; dadas las cambiantes condiciones y las nuevas plataformas de sistematización disponibles que posibilitan interconectarse a través de redes, abriendo nuevos horizontes para permitir explorar más allá de las fronteras de la compañía. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas de información. Por ello se hace más necesario proteger la información relevante de las compañías; bajo la óptica de integrar los sistemas de información y utilizar lenguajes cercanos al negocio de las organizaciones, para lo cual debe estar sincronizado, armonizado y con un plan de seguridad entre los procesos de una compañía con el fin de brindar confianza frente al negocio.

La seguridad informática, es la aceptación clara de cada uno de los usuarios del sistema informático de la compañía, en conocer las PSI, herramienta que permite adoptar una cultura de seguridad informática, orientado a proteger el activo informático y estratégico de la compañía, los cuales deben estar alineados con los objetivos del negocio y los criterios

de seguridad informática considerados por *El Information Technology Evaluation Criteria* (ITSEC)" mencionados por: (Romero 2003 p.35). Que para la seguridad informática se debe tener en cuenta como:

- ✓ **La integridad:** consiste en garantizar que los datos sean los reales y que el activo no ha sido alterado de manera no autorizada**.**
- ✓ **Confidencialidad:** garantizar que la información sea accedida solo por personal debidamente autorizado y tengan acceso a los recursos que se intercambian.
- ✓ **Disponibilidad:** garantizar que la información siempre esté disponible para el usuario que lo requiere o final.
- ✓ **Privacidad:** los componentes del sistema son accesibles solo para el personal debidamente autorizado.
- ✓ **No repudio,** garantizar de que no puedan negar una operación realizada o no pueda alegar desconocer el hecho.
- ✓ **Autenticación**: asegurar que el acceso a los recursos del sistema informático, solo se realice por personal autorizado y asegura el origen y destino de la información.
- ✓ **Control**: asegurar su conformidad con la estructura de seguridad informática y procedimientos establecidos por la compañía en cuanto el acceso a la información y el monitoreo de los usuarios autorizados.
- ✓ **Auditoria:** determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema comprobando la idoneidad de los controles.

El Universal en su artículo Tendencias para la Seguridad Informática para el 2014, escrito por: Raphael La Baca Castro, dice: "La falta de concientización sigue siendo uno de los principales obstáculos al momento de proteger adecuadamente la información y privacidad del usuario en Internet. En una primera instancia es la propia persona quien decide qué información publicar y qué no, por ende, también puede aumentar o disminuir el nivel de su privacidad en Internet" (La Baca 2014 p.1)**.**

2.2.2. Sistema de Gestión de la Seguridad de la información.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta estratégica que ayuda a las compañías a implementar políticas de seguridad informática, procedimientos y controles de seguridad informática alineados con los objetivos del negocio, con el fin de evaluarse y tener una visión global sobre el estado de los riesgos y estos sean conocidos, asumidos, minimizados y gestionados por la compañía de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la compañía, en cuanto a los riesgos, el entorno y las tecnologías a lo largo del tiempo.

La implementación de un Sistema de Gestión de Seguridad de la Información permite establecer un proceso de mejora continua a través del seguimiento de un modelo PHVA (Planear, Hacer, Verificar, Actuar), para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información, con unas responsabilidades claras y el compromiso manifiesto por parte de directivas (NTC-ISO/IEC 27001, 2006). En cuanto al (SGSI, CAVIEDES y PRADO, 2012) piensa de igual manera.

2.2.3. Seguridad informática en bases de datos.

La seguridad informática en una base de datos es crítica, debido a que se podría considerar como la caja fuerte de una compañía, en donde la mayoría de la información es sensible y de mucha importancia por guardarse las transacciones financieras de la compañía. Una base de datos se puede definir como una recopilación de información sobre diversos aspectos tales como: personas, productos, pedidos, contabilidad, transacciones, etc. Por lo cual se debe contemplar un buen plan de seguridad informática para que sea efectiva, para ello necesita contar con elementos indispensables de apoyo: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.

Ante la necesidad de manejar grandes volúmenes de información y compartir con un conjunto de clientes a través de una interfaz única y bien definida de una manera segura, surgen los servidores de base de datos, quienes tienen el control sobre los datos a través de un programa que provee servicios de base de datos a otros programas de aplicación de gestión de base de datos u otras computadoras (servidores), dedicadas a ejecutar programas que prestan el servicio, definido por el modelo o arquitectura cliente-servidor.

Los sistemas de administración de base de datos (SGBD), son aplicaciones proveen funcionalidades para servidores de base de datos, y como tal deberá ofrecer soluciones seguras de confiabilidad, rentabilidad y de alto rendimiento (VEGA (2012 p 64)

Teniendo en cuenta los riesgos a los que puede estar sometida una base de datos, es muy importante identificar y asegurar los servidores que contiene las bases de datos más sensibles y buscar alternativas para proteger las posibles amenazas, eliminado las vulnerabilidades para minimizar los riesgos que pueden estar sometida la información.

2.2.4. Seguridad Informática en aplicaciones web.

El crecimiento exponencial que ha tenido el *Internet*, las Telecomunicaciones, el mundo digital y el desarrollo económico, quienes exigen que toda la oferta cumpla la demanda del mercado, por ello cada vez aparecen más tiendas en línea, negocios que mueven grandes cantidades de dinero, redes de los servicios que habilitan el comercio a nivel internacional, así como sitios de redes sociales que contienen información muy delicada de la vida privada de sus miembros.

La necesidad de implementar la seguridad informática en los procedimientos usados para compartir la información se vuelve más importante principalmente las piezas que intervienen de forma directa con las masas de usuarios y el desarrollo de aplicaciones *web*. Ante esto es primordial abordar la seguridad informática en redes de telecomunicaciones, sistemas operativos e informática forense. Es por ello que el tema de seguridad informática se debe asimilar como un engranaje en el que intervienen muchas áreas y técnicas cuando se trata de proteger la integridad de la información y la privacidad de los datos de los usuarios.

La seguridad informática se fundamenta en conceptos y mecanismos utilizados para la detección de vulnerabilidades en aplicaciones web, teniendo en cuenta que (TARAZONA 2013 p9). Dice que:

> Las áreas críticas del diseño de aplicaciones *web* demostrarán que van desde la misma infraestructura en telecomunicaciones, el entorno de implementación, hasta el código c y los lenguajes de programación usados para la puesta en marcha de las aplicaciones *web*. Todo es

parte de un ciclo de vida de desarrollo *web* pero teniendo en cuenta aspectos de seguridad que protegen la forma y el fondo de las aplicaciones. No se trata de diseñar e implementar aplicaciones que solo den una buena imagen y gusto al cliente, sino también aspectos de seguridad que minimicen el riesgo de pérdida de información o de manipulación de la misma.

El protocolo HTTP, el modelo TCP/IP cuenta con diversos protocolos en su capa de aplicación: HTTP, SMTP y FTP son tres de los más importantes. En principio, cualquiera de ellos puede ser utilizado para la transferencia de mensajes SOAP, pero HTML es el protocolo estándar para la *web* y el más usado en los servicios *web* XML.

Figura No. 1. Modelo OSI. Fuente: Ing. Carlos Alberto Amaya Tarazona. 2013. Duitama. Seguridad en aplicaciones Web. Universidad Nacional Abierta y a Distancia

En la anterior figura No. 1, se observa los diferentes protocolos que actúan en las capas de modelo OSI, estos presentan deficiencia de diseño generando vulnerabilidad que afectan las características de las aplicaciones *WEB* como la integridad, disponibilidad y confidencialidad.

2.2.5. Seguridad informática en redes.

La Seguridad informática en Redes es un nuevo campo del conocimiento, surgido de la integración de las tecnologías de las comunicaciones y la computación, propiciado por el rápido desarrollo de las tecnologías de la información y con ello el tema de seguridad informática de las redes de comunicación que permiten el funcionamiento armónico de diferentes procesos al interior del país y de los sitios de trabajo y estudio.

Los principales aspectos de seguridad informática en redes son: disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, considerando junto a los componentes de la red como: *Switches, Routers, firewall, IPS/IDS, Gateway Antivirus*, etc. Que combinados e integrados de una forma estratégica y efectiva aseguran la red y por ende la seguridad de la información.

La seguridad informática de la red es una responsabilidad de los administradores, de mantener actualizado las aplicaciones, el equipo de trabajo incluido el usuario final, actualización de Antivirus y configuración correcta del sistema operativo, por el cual se puede dejar el sistema vulnerable a cualquier intruso (Palta 2012).

2.2.6. Identificación de activos: el corazón del negocio.

El objetivo de toda compañía es buscar Estrategias de Seguridad para proteger la Información y los activos de información, que generalmente son dependientes los activos de los servicios y procesos de negocio de la compañía.

En la actualidad, las actividades, servicios o procesos del negocio desarrollados por una compañía, dependen de la información y los medios empleados para su procesamiento, almacenamiento o trasmisión y cuando uno falla, supone un impacto en las actividades de la compañía.

El modelo de análisis y gestión de riesgos tiene como objetivo identificar los riesgos a los que se encuentran sometidos los activos de información, para ello debe realizarse un inventario de los servicios de seguridad informática, los procesos implicados y los activos de información que dan soporte a dichos procesos, de forma que la compañía pueda priorizar los mismos y adoptar las medidas adecuadas para protegerlos de acuerdo al mapa de activos sobre el cual se desarrollará el posterior análisis de riesgos. Este modelo también identifica las amenazas y vulnerabilidades a las que se encuentran sometidos los activos de información. En caso de materializarse una determinada amenaza en forma de incidente de seguridad informática, en impacto tendría doble vertiente:

- ✓ En primer lugar, afectará al propio activo de información, en forma de degradación o pérdida del mismo.
- ✓ En segundo lugar, la degradación o pérdida de un activo afectará a los procesos de negocio que lo utilizaban y, por ende, a los servicios proporcionados por la compañía.

Es decir, las amenazas se materializan, explotando las vulnerabilidades, en los activos de información, mientras que el impacto repercute en los servicios y procesos de negocio. Los activos de información tienen un valor de acuerdo a su importancia desde la perspectiva de los servicios y procesos de la compañía (MEGIAS 2008)

2.2.7. Plan de Contingencia.

El plan de contingencia es un procedimiento alternativo para el desarrollo normal de las actividades de la compañía, aunque algunas de sus funciones se hubiesen dañado por accidentes internos o externos; tener un plan de contingencia no significa que reconozca la ineficiencia de la compañía, por el contrario es estar preparados, para superar cualquier eventualidad que pueda acarrear pérdidas materiales, de información y personales, con el fin de hacer frente a futuros acontecimientos para lo cual se debe estar preparados con el único fin de dar continuidad a las actividades de la compañía.

Para la elaboración de un buen Plan de Contingencia se debe dividir en cuatro etapas, las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro:

- ✓ **Evaluación**. Los responsables de la Planificación, deben evaluar constantemente los planes creados, del mismo modo deberán pensar en otras situaciones que se pudiesen producir.
- ✓ **Planificación.** Teniendo en cuenta la probabilidad y el impacto de los riesgos existentes en la compañía, los cuales pueden causar un siniestro, sirviendo este como punto de partida para planificar las respuestas en caso de emergencia, se debe trabajar con hipótesis y desarrollar los posibles escenarios de solucionar la emergencia.

- ✓ **Pruebas de viabilidad**. Se trata de demostrar cada uno de los procedimientos que se están utilizando estén completos y de acuerdo a lo establecido, los recursos materiales están disponibles, para cuando estos se vayan a utilizar; las copias sean actualizadas y estén disponibles, y cada uno de los empleados participantes del grupo se encuentren preparados. Además, se debe documentar cada una de las pruebas que se realice y se tenga planeado, determinar el procedimiento de cada prueba, ejecutar cada una de las pruebas documentadas en base a los resultados obtenidos, actualizar el plan de contingencia de acuerdo a los procedimientos y calendarios de mantenimiento establecidos.
- ✓ **Ejecución.** Cuando un siniestro se materializa, el grupo de contingencia, debe regirse al plan de contingencia diseñado y los procesos planeados y validados, dando respuesta inmediata para dar continuidad a los servicios informáticos.

Entre los programas de implementación de la seguridad informática se debe tener diseñado un buen plan de contingencia que a la compañía le permita salvaguardar sus activos de información con las siguientes características:

- ✓ **Aprobación**: el plan debe ser aprobado por la dirección y aceptado por los usuarios y la auditoria.
- ✓ **Flexibilidad:** no debe presentar situaciones individuales de desastre, debe estar especificado mediante guías.
- ✓ **Mantenimiento:** debe ser fácilmente actualizable y evitar especificar al mínimo detalle.
- ✓ **Costo-efectividad:** la proporción de inversión entre las medidas a aplicar y las ventajas que se conseguirán deben ser justas y razonables.
- ✓ **Repuesta organizada:** la respuesta a un plan de emergencia inmediata debe proporcionar una lista de acciones y servicios ante el desastre, para ello se debe incluir listas de teléfonos y direcciones de individuos involucrados en el plan, para poder contactar con ellos.
- ✓ **Responsabilidad:** las responsabilidades asignadas a cada individuo determinada en las funciones como respuesta al plan.

Los factores a tener en cuenta para la implementación de un plan estratégico se enumeran a continuación: establecimiento de un equipo organizado de personas, preparados y listos para actuar en caso de hacerse efectivo el plan; una adecuada metodología de actividades que permitan a la compañía restablecer las funciones misionales; realizar un análisis del negocio de la compañía teniendo en cuenta sus funciones, objetivos y misión de la compañía; la inversión presupuestal destinada a un plan de emergencia depende de las áreas financieras de las compañías e instituciones que vigilan el destino del presupuesto, el cual debe estar bien sustentado.

2.3. MARCO CONTEXTUAL

Para el desarrollo del presente proyecto para optar el título de especialista en seguridad informática, se utiliza una compañía, encargada de prestar un servicio público a la comunidad nariñense y que por efectos de seguridad de la información se le dio el seudónimo de PROPOLSINECOR S.A.

PROPOLSINECOR cuenta en el momento con una infraestructura de 25 servidores, para cada una de las Bases de Datos y las aplicaciones que manejan las diferentes áreas de la compañía, 331 equipos de cómputo de escritorio y 41 equipos portátiles, utilizando medios de comunicación como: fibra óptica, cable UTP, radioenlace por microondas y por red telefónica, entre sedes ubicadas en diferentes partes del departamento de Nariño. El estudio se realiza únicamente para el área comercial que cuenta con 90 usuarios del sistema de información comercial y que poseen información heterogénea.

2.4. MARCO LEGAL

El caso de estudio se basa en los soportes teóricos y prácticos de estándares normativos, metodologías y buenas practicas que establecen los principios para el uso eficaz, eficiente y aceptable en las tecnologías de la información, ayudando a los directores a equilibrar riesgos y oportunidades con el único objetivo fundamental de proteger la información de la compañía para que no caiga en manos incorrectas o se pierda.

2.4.1. Estándares normativos.

Los estándares normativos más destacados para la implementación de la seguridad informática están:

- ✓ **ISO 27001-2005**. Estándar Internacional proporciona un modelo para: establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una compañía. Permite evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información.
- ✓ **ISO 27002.** Recopilación de buenas prácticas para un SGSI en la compañía la cual contiene recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una compañía y describe los aspectos a analizar para garantizar la seguridad de la información y especifica los controles y medidas recomendables a implementar.
- ✓ **ISO 27005-2008**. Establece las directrices para la gestión del riesgo en la seguridad de la información. para lo cual previamente se debe tener conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad de la información.

2.4.2. Leyes y decretos Colombianos.

Las leyes, resoluciones y circulares creadas en Colombia en pro de la protección de los medios informáticos, la información y el comercio electrónico, se destacan los siguientes:

- ✓ **Ley 527 de 1999 - COMERCIO ELECTRÓNICO** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”
- ✓ **Ley 962 de 2005.** Con esta Ley invita a los organismos, que ejercen funciones públicas a utilizar medios tecnológicos integrados con el apoyo del ministerio de comunicaciones, para disminuir tiempos y costos en la realización de gestiones

administrativas, aplicando los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa y deberá garantizar los principios de autenticidad, disponibilidad e integridad. Para el efecto, podrán implementar las condiciones y requisitos de seguridad informática que para cada caso sea procedentes, sin perjuicio de las competencias que esta materia tengan algunas entidades especializadas. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos (GALLO 2005).

- ✓ **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, como penas de prisión de 120 meses y multa de hasta 1500 salarios mínimos legales mensuales vigentes. La ley castiga los atentados contra la confidencialidad, la integridad y la confidencialidad de los datos y de los sistemas informáticos, entre otras infracciones como hurto por medios informáticos y semejantes, transferencia no consentida de activos y circunstancias de mayor unidad (ANDRADE 2009).
- ✓ **Ley 1341 de 2009.** La presente ley, determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información (GUERRA 2009).

- ✓ **Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009.** Sobre seguridad informática de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad informática, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad informática de sus redes de acceso, de acuerdo con los marcos de seguridad informática definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información (GUERRA 2009).
- ✓ **Circular 052 de 2007 (Superintendencia Financiera de Colombia).** Fija los requerimientos mínimos de seguridad informática y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios, bajo los siguientes **Criterios de Seguridad de la información (SIFC 2007)[10]:**
  - a) **Confidencialidad:** Hace referencia a la protección de información cuya divulgación no está autorizada.
  - b) **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

[10] La Súper Intendencia Financiera de Colombia. CIRCULAR EXTERNA 052 DE 2007. Capitulo Décimo Segundo: Requerimientos Mínimos De Seguridad y Calidad en el Manejo de Información a Través de Medios y Canales de Distribución de Productos y Servicios. Entra en vigencia mediante tres etapas: la primera inicia el 1º de julio de 2008, la segunda el 1º de enero de 2009 y la ultima el 1º de enero de 2010.

- c) **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

y bajo los siguientes Criterios de Calidad de la información.

- a) **Efectividad:** La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- b) **Eficiencia:** El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- c) **Confiabilidad:** La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

- ✓ **Ley 1581 de 2012 y del Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.** La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C–748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión, en adelante tratamiento por parte de entidades de naturaleza pública y privada. Como Ley Estatutaria (ley de especial jerarquía), tiene como fin esencial salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección (CERTICAMARA 2012)[11].
- ✓ **Decreto 1151 de 2008.** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.

[11] CERTICAMARA. ABC para proteger los datos personales Ley 1581-2012 decreto 1377 de 2013. https://www.certicamara.com

2.4.3. Leyes internacionales.

Internacionalmente existen Leyes que regulan la seguridad informática de las organizaciones en el Esquema Nacional de España como el siguiente caso:

- ✓ **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.** El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el **artículo 42 de la Ley 11/2007, de 22 de junio**, y determinar la política de seguridad informática que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada Ley. El Esquema Nacional de Seguridad informática está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. La ley en el capítulo II. Principios básicos, **Articulo 4 Principios básicos del Esquema Nacional de Seguridad Informática**. El objeto último de la seguridad de la información es asegurar que una compañía administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad para los cual debe tenerse en cuenta cinco (5) principios básicos: a) Seguridad informática integral, b) Gestión de riesgos, c) Prevención, reacción y recuperación, d) Líneas de defensa, e) Reevaluación periódica, f) Función diferenciada.
- ✓ Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad informática, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad informática, se establecerá en base a los principios básicos en la implantación de seguridad informática (REY DE ESPAÑA 2007).
    - ➢ El análisis y gestión de riesgos será parte esencial del proceso de seguridad informática y deberá mantenerse permanentemente actualizado.

- La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad informática, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad informática.
- Cada compañía que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.
- Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna metodología reconocida internacionalmente.
- En el sentido formal de autorización para manejar información clasificada. Los procesos de acreditación se ajustan a la normativa aplicable en cada caso.

3. METODOLOGIA

3.1. PARADIGMA DE LA INVESTIGACIÓN

Investigación cuantitativa: la investigación se llevó a cabo bajo el enfoque cuantitativo considerando que se estudian variables susceptibles de cuantificación y medición con indicadores objetivos.

3.2. TIPOS DE INVESTIGACIÓN

La presente investigación es descriptiva ya que se aborda la seguridad informática y los principales riesgos de seguridad informática que tiene PROPOLSINECOR; también una investigación aplicada, orientada hacia la gestión de sistemas y en busca de generación de soluciones a los problemas que se encuentran en la compañía. Adicionalmente puede caracterizarse como propositiva en vista de que se genera como producto una propuesta de políticas de seguridad informática.

3.3. DISEÑO INVESTIGACIÓN

El diseño empleado en la investigación fue no experimental de tipo transaccional o transversal; porque no se manipuló intencionalmente ninguna variable, los resultados se fundamentan en la observación y análisis descriptivo de lo encontrado. Además, no incluye el seguimiento a la aplicación de las políticas de seguridad informática propuestas.

El proyecto se desarrolló mediante las siguientes actividades:

- ✓ Mediante herramientas seguridad informática se analizó las vulnerabilidades y amenazas que existen en los sistemas de cómputo, comunicaciones y red intranet.
- ✓ Mediante encuestas a los usuarios del sistema informático y entrevista a los responsables de los sistemas de cómputo, se diagnosticó la aplicación de los estándares de seguridad informática en la red, servidores y usuarios en general y se realizó un análisis de las políticas se seguridad informática implementadas en la compañía.

El análisis de riesgos en seguridad informática se llevó a cabo mediante el reconocimiento del estado de la seguridad del sistema informático con el fin de modelarlo, identificando y valorando amenazas informáticas sobre los activos. Así pues, se pudo estimar el riesgo a que el sistema está expuesto. Para mitigar los riesgos se propone políticas de seguridad informática.

3.4. POBLACIÓN Y MUESTRA

Población

Personal de PROPOLSINECOR, que está involucrado con la administración o seguridad informática como los administradores de los diferentes aplicativos y base de datos existentes en la compañía, usuarios del sistema de información comercial y financiero.

Muestra

Teniendo en cuenta el objetivo de la investigación y las características de la población se procedió mediante una muestra intencionada (No estadística). Se realizó entrevistas a ocho (8) Administradores, quienes se seleccionaron bajo el criterio de responsabilidad frente a las funciones de seguridad informática en la administración de base de dados y aplicativos de la compañía. Dado que la empresa cuenta con ocho administradores, la recolección de información se hizo sobre el 100% de este sector de la población. En cuanto a los usuarios de los sistemas comercial y financiero, quienes suman 90 personas, se optó por aplicar un censo buscando conseguir mayor validez de la información recolectada, partiendo del supuesto de que todos no aceptarían colaborar con la investigación ya que se trata de un tema delicado y sensible, y los usuarios son esquivos y celosos con la información pues no les gusta ser cuestionados en el manejo de la información que tiene bajo su responsabilidad. Se envió la encuesta por correo corporativo y como resultado se obtuvo que 41 personas contestaran voluntariamente. Esta información se consideró suficiente y se continuó a las fases siguientes.

3.5. FUENTES DE INFORMACIÓN

Las fuentes de información que se tienen en cuenta para la realización del proyecto se pueden catalogar en información primaria y secundaria.

- ✓ **Fuentes de información primaria.** Las fuentes primarias están constituidas por la información original suministrada por los profesionales administradores de aplicaciones y Bases de Datos de la compañía; hechos acaecidos a la seguridad informática y a la infraestructura de PROPOLSINECOR.
- ✓ **Fuentes de información secundaria.** La información secundaria es toda la información documental que orienta al análisis y evaluación de la seguridad informática y que se encuentra consignada en documentos como: normas: NTC- ISO-IEC-27001, NTC- ISO-IEC-27002 y Metodología MAGERIT, modelos de seguridad informática COBIT y documentos de la compañía.

3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Entrevista: para obtener información relevante para el proyecto se utilizó la entrevista de modelo conversacional, por ser una técnica eficaz para obtener datos relevantes y significativos, utilizando una entrevista no estructurada con el fin de obtener una opinión personalizada de los Profesionales Universitarios y Especializados quienes son los encargados de la administración de las aplicaciones, base de datos y comunicaciones.

Encuestas: para determinar vulnerabilidades, conductas y conocimiento que tenían los usuarios de las políticas de seguridad informática, se aplicó una encuesta que fue contestada por 41 personas.

Observación: por otra parte en la realización del proyecto se utilizó la observación para registrar patrones de conducta de los usuarios y del sistema informático.

Revisión documental: para ello se revisó los documentos existentes que brindan soporte a la seguridad informática y el control de los mismos como son: normas NTC-ISO-IEC-27001, NTC-ISO-IEC-27002, NTC-ISO-IEC-27005, Metodología MAGERIT y

documentación de PROPOLSINECOR que soportan SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION".

Herramientas: para realizar la recolección de información se utilizó grabadora herramientas de google drive y para el análisis herramientas de office (Excel)

4. RESULTADOS

4.1. ACTIVOS DE INFORMACIÓN Y DE NEGOCIO EN LA COMPAÑÍA

Para identificar los activos de información se realizó entrevistas, encuestas, revisión de documentos institucionales y archivos operativos o de soporte, planes para la continuidad del negocio, investigación, manuales de usuario, material de formación y observación directa.

4.1.1. Información que se maneja.

- **Información financiera.** Según el responsable de la administración, la información se maneja mediante un aplicativo que se encuentra en desarrollo y existen varios módulos jerárquicos, que responsabilizan a las diferentes oficinas involucradas del manejo y responsabilidad de la información contenida en la base de datos, se puede clasificar dependiendo del módulo que en general, contiene información de carácter financiero y de carácter personal, como: nómina de la compañía que contiene información de los empleados como el pago y los descuentos por libranza e información clasificada, contratos de la oficina jurídica e información pública como los estados financieros de la compañía.
- **Información comercial (facturación)**. Se maneja la facturación del servició público y base de datos de los clientes, la cual contiene registros confidenciales de cada factura como: reclamos, cartera, créditos, pagos, abonos, muchos otros registros y procesos de control y atención en la facturación de la compañía, todo esto manejado por una aplicación a cargo de un contrato de una compañía de subcontrata (*Outsourcing*).
- **Información específica y técnica de la compañía.** Para el control de procesos que involucra indicadores estadísticos de eficiencia y calidad del servicio público prestado por la compañía, los cuales deben ser reportadas a los entes regulatorios del negocio, quienes sancionan con devolver dinero a los clientes afectados por mala calidad, por ausencia del servicio público o incumplimiento a indicadores asignados por las normas

regulatorias del negocio. Además, algunos registros de la base de datos se encuentra en sincronía con la información de facturación, la cual permite realizar cálculos técnicos que permiten ofrecer un servicio eficiente y de calidad al usuario final. Además, se está automatizando el control de servicio público prestado, tanto a las fuentes como a los usuarios finales, con el fin de garantizar la continuidad del mismo.

- **Información de seguimiento a las metas corporativas**. Llamado también como cuadros de mando para el control y seguimiento de los procesos, proyectos de trabajo asignados a cada departamento, facturación, recuperación de cartera, atención al usuario, gastos administrativos entre otros; todo esto con el único objetivo de que los responsables tengan un indicador de control de sus metas que deben cumplir para la mejora continua, la excelencia y calidad del servicio público prestado al usuario final.
- **Administración documental**. Para la administración documental existe un aplicativo que maneja base de datos, donde reposa la correspondencia interna o externa en medio digital, incluidos los mensajes entre los usuarios de la compañía, permitiendo realizar un seguimiento al documento mediante un número de radicado hasta su respuesta o solución final. Además, la información documental que soportan todas las actividades de la compañía están almacenadas en el centro de administración documental, el cual está destinado a proteger y mantener una logística que permite consultar los documentos requeridos en un tiempo eficiente. La documentación que representan un gran valor, ya sea por su confidencialidad o de valor económico para la compañía, están archivados en una compañía de seguridad de valores.
- **Información del sistema de gestión de seguridad informática**. Estos documentos forman parte integral de la documentación de gestión de calidad, implementado por la compañía en un aplicativo de gestión de procesos de la norma NTC ISO 9001 y son una guía para el usuario en la protección de la información sensible, para lo cual se realizó un inventario de la documentación guía existente y se realiza una descripción de cada documento como consta en el anexo No. 1.
- **Información de administración y configuración de las comunicaciones**. Esta información forma parte de los diferentes elementos de control de hardware instalado

en las comunicaciones a responsabilidad de la oficina de Planeación y Sistemas. Además, existe un plano estructural de la red existente en la compañía, en la cual se plasma sus componentes, configuración y conexiones entre las redes de la compañía. Esta información reposa en la oficina del administrador de la red de comunicaciones, pero el control de la seguridad informática, el mantenimiento de la estructura y configuración de la red está a cargo de terceros, que actualmente se encuentra realizando cambios estructurales en la configuración e implementando redes lógicas por áreas, con la segmentación por medio de VLAN, para mejorar la seguridad informática.

4.1.2. Bases de datos y más datos.

Las bases de datos que se pudieron identificar en la compañía son de tipo dinámicas por procesar información que se está modificando diariamente y estáticas por guardar información histórica, entre ellas se pueden destacar:

- **Base de datos para procesar información financiera y administrativa.** Considerada como muy sensible y de alto valor, en el momento se encuentra en proceso de implementación de una nueva base de datos en sincronía con una base de datos espejo, instalada en un segundo servidor de respaldo, en donde se realizan todo tipo de transacciones financieras y contables de egreso e ingreso para la obtención de estados financieros de la compañía; estas bases de datos en *Oracle 11G* es administrada en conjunto con el aplicativo que se encuentra en desarrollo por el mismo profesional especializado del departamento financiero. El administrador en la entrevista manifiesta que hace falta más profesionales para la administración.
- **Base de datos de información comercial.** Instalada en el mismo servidor del aplicativo administrado y configurado por un subcontrata (*Outsourcing*), en ella se realizan todos los procesos que involucre al usuario, como la información básica del cliente, información de atención al usuario, cartera y módulos de control del servicio ofrecido, administrada por un profesional de la firma contratada.

- **Base de datos documentales.** Esta base administra la información documental que debe tramitarse en la compañía a nivel interno y externo, instalada en el mismo servidor del aplicativo, pero en sincronía con un servidor espejo de respaldo que entra en funcionamiento inmediatamente falle el principal.
- **Base de datos cuadros de mando.** Esta base hace interfaz con todas las bases de datos de la compañía como: la base de datos financiera, facturación, información de control de calidad, de producción, actividades propias de la compañía, control o avance de proyectos, lo que permite tener el control de metas que se están logrando por cada dependencia.
- **Base de datos de servicios distribuidos a otros comercializadores.** Los cuales se controlan en una base de datos independiente y administrada por el profesional de sistemas, e instaladas en el mismo servidor, lógicamente con su servidor de respaldo.
- **Base de datos de información técnica**. En cumplimiento de normas regulatorias del negocio es necesario tener información de la estructura técnica de distribución y comercialización del servicio público e información estadística de control de calidad, continuidad del negocio, control remoto de la prestación del servicio para mantener la eficiencia y continuidad; esta información es valorada por la entidad regulatoria del negocio, quien tiene establecido metas de calidad y continuidad en la prestación del servicio público, que influyen directamente en el valor de la tarifa final del servicio público prestado al usuario final.

- **Copias de respaldo.** Existe un procedimiento de sacar copias de respaldo diario, semanal y mensual, para entregar en custodia a una compañía de protección de valores contratada por la compañía, para ello existen formatos de control y custodia de copias de seguridad del sistema financiero, comercial, e información sensible de la compañía.
- **Datos de configuración.** La información de configuración de los servidores es manejada por los proveedores del aplicativo o base de datos y la de los pc de escritorio y portátiles son responsabilidad de la oficina de sistemas.

- **Datos de gestión interna.** La información de gestión interna, como el cronograma de mantenimiento, configuración de estaciones de trabajo, entre otras. Son administrados y elaborados por la oficina de sistemas.
- **Credenciales / contraseñas.** Cada aplicativo maneja su propia política de seguridad informática en el control de la creación y administración de contraseñas. El aplicativo del sistema de información comercial tiene un módulo de auditoria administrada por la oficina de control interno quienes gestionan los perfiles y contraseñas de los usuarios, esta es asignada y vence cada quince días y faltando seis días mediante un mensaje al usuario, avisa de su cambio. Además, si el usuario digita equivocadamente tres veces una contraseña errónea, la sección del usuario queda bloqueada y tiene que gestionarse una nueva contraseña ante la oficina de control interno.
- **Datos de control de acceso.** Existe un procedimiento parcial de control de acceso a las aplicaciones, pero no hay un procedimiento estandarizado adecuado. Cada administrador lo controla a su manera dependiendo de su conocimiento y experiencia, pero no existe procedimientos que responsabilicen a una oficina sobre quien debería informar a cada administrador el ingreso o terminación del contrato de un usuario, con el fin de que el administrador tenga la responsabilidad de crear o dar de baja los derechos de acceso a las aplicaciones que maneja.
- **Registro de actividad.** Según los entrevistados, la mayoría de los sistemas de información tiene configurado los *logs* de registro de actividades, pero no existen profesionales encargados de hacer el seguimiento de las actividades de los diferentes usuarios de la compañía. El sistema financiero con el aplicativo en desarrollo han contemplado horarios de acceso a la información que va desde las 7:00 AM a las 7:00 PM. Otro aplicativo que tiene contemplado horario de acceso solo con el módulo de recaudo es el sistema comercial, el cual tiene el mismo horario del sistema financiero.

  Los administradores consideran que debe existir más profesionales encargados de hacer auditorías a los diferentes módulos de información principalmente a los usuarios con perfiles de borrado y modificación de la información.

- **Código fuente.** El código fuente esta manejado por los diferentes proveedores del software y encargados de estar actualizando los requerimientos propios de la compañía, esto para los aplicativos a la medida y que son distribuidos por casas comerciales. Los aplicativos propios de la compañía y los códigos fuente, se encuentran copia en la oficina de sistemas y la compañía de valores contratada.
- **Código ejecutable.** El código ejecutable se encuentra instalado en los servidores y diferentes módulos o estaciones de trabajo y los instaladores son manejados directamente por los administradores de los aplicativos con copia en caja de valores y proveedores del software.
- **Datos de prueba.** En las aplicaciones a la medida que se realizan pruebas a los módulos modificados o creados, estos son probados con una copia de la base de datos principal, residentes en un servidor de pruebas, con el fin de demostrar la funcionalidad y validación del módulo al grupo interventor del contrato y la oficina solicitante, quienes aprueban la puesta en producción.
- **Herramientas de navegación Internet**. En la arquitectura de red está el correo corporativo y la navegación abierta por el mundo del ciberespacio con muy pocas restricciones para la mayoría de los usuarios del sistema de la compañía.

4.1.3. Claves criptográficas.

La compañía no utiliza ningún tipo de protección de la información con claves criptográficas, las bases de datos son encriptadas con la seguridad informática que traen por defecto o se pueden configurar en su creación.

4.1.4. Software.

- **Software de sistema operativo**. Los sistemas operativos utilizados en los servidores son: *Solaris* y *Windows server*; los computadores de escritorio utilizan una variedad de sistemas operativos en versiones de *Windows*, como *Windows XP*, *Windows 7* y *Windows 8*.

- **Software de aplicaciones estándar, de desarrollo propio y desarrollo a medida**. La mayoría de las aplicaciones que manejan la información mencionada en los activos de datos e información es software a la medida, esto ha permitido a la compañía emprender una solución a sus problemas y necesidades, con herramientas tecnológicas de última generación, para mejorar la eficiencia de sus procesos de negocio, las cuales están ajustadas a la medida de las necesidades de la compañía.
- **Software para el manejo del sistema financiero.** Este aplicativo se encuentra en desarrollo y existen varios módulos que gestionan la información exclusiva de un área como son: almacén, compras, contabilidad, tesorería, presupuesto, jurídica entre otras, la cual se encuentra administrada por un profesional especializado a contrato indefinido.
- **Aplicativo para el manejo comercial de la compañía.** Aplicativo a la medida de la compañía y administrada por un subcontrata (*outsourcing*), el cual maneja varios módulos que involucra diferentes áreas de la compañía, como la facturación, críticas a la facturación, atención al cliente, cartera, recaudo, etc. Administrada por un tercero, profesional vinculado al subcontrata *outsourcing*, vigilado por un grupo de dos interventores los cuales tienen asignadas muchas otras actividades del cargo.
- **Aplicativos que manejan actividades técnicas y específicas.** Estas aplicaciones no pueden ser reveladas por confidencialidad de la compañía, las cuales son administradas por profesionales con contrato indefinido y contratos a término fijo. El soporte y la administración de la aplicación están a cargo del proveedor de la aplicación.
- **Aplicativo en ambiente web para los cuadros de mando.** Este aplicativo es administrados por un profesional de la compañía a término indefinido, el cual tiene enlaces de consulta con las base de datos de la información, para realizar seguimiento a las metas y proyectos de la compañía, además contiene cada uno de los procesos que involucra la calidad del negocio y servicio que presta la compañía.
- **Aplicativo de administración documental**. Administrada por un profesional a contrato fijo, en este aplicativo se radica todo documento interno y externo que requiere trámite en la compañía, ya que existe la política de seguridad informática de no tramitar ningún documento que no haya sido radicado por este aplicativo.

- **Software de Utilidades.** La compañía no utiliza ningún *software* de utilidades distinto al que viene o se instala con el sistema operativo en cada uno de los pc y los servidores.

4.1.5. Servicios que presta.

Los servicios que presta la compañía se pueden clasificar de la siguiente manera:

- **Anónimo y al público en general (sin requerir identificación del usuario y sin relación contractual).** Ingresando a la página web de la compañía, puede consultar la tarifa del servicio, la última factura, noticias referentes al servicio prestado, reglamento de contratación y prestación del servicio, publicación de invitaciones a contratación de prestación de servicios técnicos y proveedores.
- **A usuarios externos (bajo una relación contractual).** Existen usuarios externos que mediante una relación contractual de proveedores de *software* ingresan a la red para brindar soporte al *software* suministrado y subcontrata (*outsourcing*), el cual tiene un contrato vigente y administra la base de datos y el aplicativo del sistema de información comercial.
- **Interno (a usuarios de la propia compañía).** Existen trescientos cincuenta y dos (352) usuarios internos que ingresan a los diferentes aplicativos de la compañía mediante contraseñas para realizar sus actividades internas propias del negocio, para mantener en sincronía el servicio público que presta la compañía a sus usuarios, siempre buscando mejorar con la capacitación continua, implementación y actualización de nuevas tecnologías.
- **Servicios de correspondencia y control documental.** Para ello la compañía tiene implementado un *software* que controla mediante un radicado, todos los documentos internos y externos que se tramitan en la compañía.
- ***World Wide Web*.** La compañía tiene contratado un *hosting* externo para albergar su sitio *web* que se encuentra publica en el *ciber* espacio informático de la internet, en la que se encuentran temas como:

- **Quienes somos:** con los siguientes subtemas: Misión y Visión, Objetivos y valores, Política de Calidad, Reseña Histórica, Estructura Administrativa Organigrama General, Nuestras Sedes, Nuestro Clientes, Mapa de Procesos y Localización de la Compañía.
- **Noticias:** con subtemas de: Actualidad, La Ciudad y Estados Financieros.
- **Productos/servicios*:*** en la que se destacan subtemas sobre: Comercialización, Servicios Adicionales, Logística de la Compañía, Administración Documental, Línea Viva y Brigadas de Atención.
- **Responsabilidad empresarial:** Se tratan subtemas de: Responsabilidad Ambiental, Política Ambiental, Capacitación y Educación Ambiental.
- **Atención usuario: s**e publican subtemas de: Normas de Servicio, Tarifas Actualizadas, Puntos y Medios de Pago, Preguntas Frecuentes, Peticiones Quejas y Reclamos, Contrato de Condiciones de Prestación del Servicio y Reglamento de Comercialización.
- **Contratación:** con subtemas de: Contratación, Avisos de Venta y Reglamento de Contratación.

- **Acceso Remoto a Cuenta Local.** Este servicio no se encuentra reglamentado dentro de la compañía y su existencia atenta contra la seguridad informática, ya que utilizan aplicaciones libres existentes en el internet.
- **Correo Electrónico.** El correo que maneja la compañía es corporativo contratado con Gmail bajo el dominio de la compañía para doscientos setenta y dos (272) usuarios de correo.
- **Almacenamiento de ficheros.** Para el almacenamiento de información de los usuarios internos de la compañía, existe un servidor de archivos, el cual está configurado por áreas con el mismo perfil, por este motivo no es seguro guardar los ficheros de carácter permanente, debido a esto es utilizado como almacenamiento temporal para transferencia de archivos o compartir información con otros usuarios de la *intranet* de la compañía de forma inmediata.
- **Intercambio Electrónico de Datos**. La compañía no maneja ningún sistema de intercambio electrónico de datos.

- **Gestión de identidades Servidor de Nombre de Dominio.** Para los usuarios de la compañía que están conectados en red *Ethernet*, se encuentran administrados bajo el dominio de un servidor de directorio de identidades.
- **Gestión de Privilegios**. Los privilegios son gestionados por los administradores de base de datos y los administradores de las aplicaciones, a excepción del aplicativo del Sistema Comercial que es gestionado por un profesional de Control Interno.
- **Infraestructura de clave pública (PKI)**. La compañía no tiene implementado ningún sistema de infraestructura de clave pública PKI, en sus sistemas informáticos.

4.2. ACTIVOS INFORMÁTICOS

4.2.1. Arquitectura del sistema.

La arquitectura de sistemas de la compañía está estructurado como Cliente- Servidor los cuales interactúan por medio de invocaciones remotas a servicios implementados en los servidores de archivos, servidores de Base de Datos, servidores de Aplicaciones, Servidor de dominio, Servidor *Web*, Servidor de correo, entre otros; por medio de una infraestructura de red que se encuentra en proceso de segmentación lógica y física formada por subsistemas claramente definidas en comunidades, para mejorar el rendimiento de la arquitectura multinivel o cliente/servidor teniendo en cuenta los siguientes puntos de comunicación como:

- **Punto de acceso al servicio.** Los puntos de acceso al servicio se están marcando con la configuración de redes lógicas mediante la creación de *VLAN* para crear comunidades, con el fin de proporcionar seguridad informática al usuario en el acceso al servicio.
- **Punto de interconexión.** En los puntos de interconexión se encuentran *router* con redundancia para garantizar la continuidad de las comunicaciones.
- **Proporcionado por terceros.** Los servicios de comunicaciones entre redes se encuentran en diferentes proveedores u operadores de comunicaciones que proveen el servicio con diferentes tecnologías.

4.2.2. Equipamiento informático (*hardware*).

Comprende todos los medios materiales y físicos, destinados a soportar directa o indirectamente los servicios que la compañía presta y son los encargados del almacenamiento y trasmisión de la información a través del sistema informático.

- **Grandes equipos (mal llamados Servidores).** En *Internet*, un servidor es un ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras, en redes locales se entiende como el *software* que configura un *PC* como servidor para facilitar el acceso a la red y sus recursos. En informática, un servidor es un tipo de *software* que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese *software*, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos y recursos. Generalmente el servidor es económicamente gravoso y requiere un entorno específico de operación. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

  En la compañía existe 25 máquinas configuradas como servidores con el fin de prestar diferentes servicios a los usuarios de la compañía, servicios que fueron analizados e inventariados en apartados anteriores, entre ellos existen servidores de respaldo, ubicados en tres cuartos diferentes dentro de la misma edificación, las máquinas que se encontraban en torres se han remplazado por máquinas en *Rack*, las cuales ocupan menos espacio.
- **Equipos medios (computadoras de escritorio).** Los equipos de escritorio se encuentran distribuidos en todos los puestos de trabajo de usuarios del sistema informático de la compañía, existen varios modelos y marcas de computadoras, con sistemas operativos en diferentes versiones de *Windows* a saber: *Windows XP*, *Windows Vista*, *Windows 7* en 32 y 64 bits, configurados bajo el dominio de la compañía. Los computadores de escritorios tienen instalado las aplicaciones propias del cargo que desempeña, algunas aplicaciones (sistema de información comercial) no se encuentran instaladas en el equipo del usuario, ya que trabajan bajo el esquema de escritorio

remoto, para lo cual tiene una maquina configurada con *Windows Server*, para que los usuarios ingresen a la aplicación por medio de esta y esté controlada y administrada por un profesional del área de sistemas.

- **Informática personal (portátiles).** Estos equipos son manejados por personal directivo de la compañía con información propia del cargo que desempeñan y generalmente ingresan a algunas aplicaciones solo para consulta, otros equipos portátiles no se conectan a la red de la compañía ya que manejan aplicaciones técnicas propias de proveedores para el mantenimiento y verificación de los servicios ofrecidos, cada uno de estos elementos es responsabilidad del usuario a quien le asignaron el activo.
- **Equipamiento de respaldo.** La compañía ha diseñado varios sistemas de respaldo para garantizar la continuidad del servicio prestado, para ello tiene varias máquinas configurados como servidores espejos en sincronía con el servidor principal de las aplicaciones y base de datos. Además, se realiza copias de respaldo a diario de la información sensible, semanal de la información menos sensible y mensual de la información propia del usuario residente en las estaciones de trabajo, estas copias son entregadas en custodia a una compañía de valores, por intermedio de la oficina de sistemas.
- **Periféricos.** Los aparatos o dispositivos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora son considerados como periféricos**,** los existentes en la compañía se podrían clasificar como:
  - **Periféricos de entrada.** Se podría decir que son los dispositivos periféricos de entrada adicionales al equipo de cómputo y que sirven para captar y digitalizan los datos, entre estos podemos destacar: el escáner que se encuentra uno por área y el escáner de barras para el personal de digitación y recaudos.
  - **Periféricos de salida**. Son dispositivos que muestran o proyectan información hacia el exterior del ordenador como: el monitor, la tarjeta de sonido y los parlantes que generalmente forman parte del equipo de cómputo, existe otros elementos de salida como el fax y las impresoras conectadas a le red *intranet* de la compañía, existen una por área u oficina para compartir con varios usuarios.

- **Periféricos de entrada/salida (E/S).** Son los que utiliza el ordenador tanto para mandar como para recibir información, estos elementos generalmente se encuentran como parte integral del equipo de cómputo como: El Disco Duro, grabadora y/o lectora de CD o DVD, unidades lectoras de USB, estos se encuentran disponibles en todos los computadores de los usuarios. La oficina de sistemas utiliza un disco duro para realizar copias de seguridad informática, que están bajo la responsabilidad de cada uno de los usuarios finales.

- **Dispositivos de frontera.** Como dispositivos de frontera se utiliza cuatro *routers*, dos se conectan a operadores proveedores de internet y dos al proveedor externo del enlace de comunicación con otras sedes que no se tiene fibra óptica, la administración y configuración a responsabilidad de la Oficina de sistemas.
- **Soporte de la red.** El soporte de la seguridad informática en la red está estructurado por elementos de comunicación que actúan en forma jerárquica en tres capas de comunicación y está administrada por los profesionales de la área de sistemas, con asesoría externa de un especialista certificado, quienes son los responsables de la administración y configuración de los equipos de comunicación como los *router*, *switch*, *firewall* y servidor *VPN*.

4.2.3. Servicios subcontratados.

Como servicios subcontratados está el *internet*, con dos puntos redundantes en la comunicación, servicio de comunicación con otras sedes del departamento de Nariño que no tiene fibra óptica y la administración de una aplicación y base de datos del sistema de información comercial.

4.2.4. Instalaciones.

Se podría clasificar en dos tipos de instalaciones como son: los servidores y equipos de comunicación que se encuentran en cuartos debidamente asegurados bajo llave física o magnética, en la responsabilidad del área de sistemas o administrador de comunicaciones, en cambio las redes están distribuidas a lo largo y ancho de las edificaciones en sectores

debidamente protegidos; los equipos de cómputo se encuentran en las oficinas y salas de digitación bajo la responsabilidad de los que trabajan en el área.

4.2.5. Redes de Comunicaciones.

La estructura de la red informática tiene un diseño jerárquico de tres capas, la cual se segmenta en grupos de comunidades de usuarios claramente definidos, la seguridad informática de acceso, constituida con veintiséis (26) *Switch* administrables en capa dos, siete (7) *routers* en capa dos y capa tres, cuatro (4) *firewall* y un servidor *VPN* instalados en sitios estratégicos para interconectar las diferentes comunidades, algunos de estos elementos son utilizados como fronteras para salir a la *internet* o establecer comunicación con otras sedes a través de los operadores de comunicaciones, quienes prestan el servicio como terceros, la responsabilidad de la administración es la Oficina de Sistemas.

- **Red metropolitana [MAN].** La compañía en su sistema informático tiene implementado una red de área metropolitana de alta velocidad (banda ancha), estableciendo cobertura de comunicación a un área geográfica extensa, cubriendo diferentes ciudades del departamento de Nariño y proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica propia y par trenzado de cobre, aplicando la norma. IEEE 802.6 *Metropolitan Área Networks*, y cuya responsabilidad de administración y manejo está a cargo de la Oficina de Sistemas con asesoría externa de un experto certificado.
- **Red digital [ISDN] *RDSI*.** Este tipo de red está formado como un servicio proporcionado por operadores de comunicaciones, los cuales permiten la comunicación con sedes donde no existe fibra propia de la compañía, cuya responsabilidad estaría en manos de terceros.
- **Red inalámbrica [*wifi*].** La red inalámbrica en las instalaciones de la compañía es muy limitada y esta implementada solamente en la oficina principal y es utilizada en sala de reuniones o el auditorio, su manejo está bajo la responsabilidad de la oficina de sistemas.

4.2.6. Personal.

Todo el personal de compañía es responsable de la protección adecuada de los activos de información existentes, y se debe tener bien claro la responsabilidad del manejo de los activos de información para implementación de controles. Teniendo en cuenta lo anterior se identifican los siguientes perfiles de usuarios en la compañía:

- **Usuarios finales (internos, externos y digitadores).** Estos usuarios del sistema informático, son responsables de la atención, recepción de peticiones, quejas y reclamos, recepción de recaudos de los clientes, facturación, ingreso y egreso de mercancía, etc. Además, actúan con cada uno de los aplicativos dependiendo del perfil que tenga como usuario del sistema informático, también son los encargados de mantener actualizada la información que manejan, cada usuario es responsable de sus actividades e información que maneja, como también del nombre de usuario y contraseña de su estación de trabajo.
- **Administradores.** Como usuarios administradores la responsabilidad es mayor, ya que son los encargados de monitorear que las transacciones y actualizaciones se realicen de acuerdo a los procesos establecidos en el manejo de información y en los servicios, avalando que la información mantenga la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, con el único propósito de mantener el control de la información, para lo cual se identifican los siguientes administradores:
  - **Administrador de comunicaciones**. Encargado de mantener la continuidad y seguridad de las comunicaciones entre los usuarios y los servicios prestados, responsable ante el directivo de la oficina de Planeación y Sistemas.
  - **Administrador de BBDD**. Existen tres administradores de base de datos responsables de la información estadística, comercial y financiera.
  - **Administrador de seguridad informática. N**o existe administrador de seguridad informática.

- **Administrador de aplicativos.** Por cada aplicativo existente en la compañía existe un administrador o encargado de mantener la aplicación disponible ante los usuarios del aplicativo.
- **Desarrolladores / programadores**. Son profesionales que se encuentran subcontratados por una compañía, que presta el soporte o mantenimiento del aplicativo generalmente externos a la compañía.
- **Subcontratas.** Existe una compañía subcontrata (*outsourcing*) que tiene la administración de la base de datos, el aplicativo incluido, el soporte y mantenimiento del sistema de Información Comercial.

4.3. VULNERABILIDADES, AMENAZAS Y RIESGOS EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN.

A partir de la información obtenida mediante las entrevistas y encuestas (ver anexo 4, 5 y 6) y a través de la observación directa se encontró las amenazas, vulnerabilidades y riesgos que se explican a continuación

4.3.1. Vulnerabilidades.

Las vulnerabilidades son puntos débiles en los procesos del manejo de activos de información, que amenazan la integridad disponibilidad y continuidad de la información sensible, la cual indica que el activo informático es susceptible a recibir un daño a través de un ataque informático, ya sea intencional o accidental, estas se pueden clasificar de acuerdo a su origen:

- **Diseño.** Los diferentes protocolos que actúan en cada una de las capas del modelo OSI presentan deficiencia de diseño generando vulnerabilidad que afectan las características de las aplicaciones como la integridad, disponibilidad y confidencialidad de la información de la compañía, esta es trasmitida a través de sus estructuras informáticas sin ningún tipo de encriptación.
  - **Debilidades en los Protocolos de red.** Debido a las debilidades existentes en los protocolos de red la compañía están en pleno proceso de segmentación, creación de

VLAN y actualizando el *Firewall*, con el único fin de asegurar y optimizar la red de la compañía; pero siempre existirán las vulnerabilidades en la red, ya que está conectada con redes externas a través de terceros, quienes prestan el servicio de internet o comunicación con las otras sedes, por eso es muy importante tener en cuenta los riesgos que se enumeran en el proyecto *OWAST Top* 10 -2013 los cuales se describen a continuación:

- A1 Inyección
- A2 Pérdida de Autenticación y Gestión de Sesiones
- A3 Secuencia de Comandos en Sitios Cruzados (XSS)
- A4 Referencia Directa Insegura a Objetos
- A5 Configuración de Seguridad informática Incorrecta
- A6 Exposición de Datos Sensibles
- A7 Ausencia de Control de Acceso a las Funciones
- A8 Falsificación de Peticiones en Sitios Cruzados (CSRF)
- A9 Uso de Componentes con Vulnerabilidades Conocidas
- A10 Redirecciones y reenvíos no validados (Williams 2013 p.5).

Estas amenazas informáticas pueden consolidarse debido a la heterogeneidad de los equipos, la integración de las tecnologías de las comunicaciones y la computación en la compañía. Analizando las respuestas en la encuesta a la pregunta. **En su computador de trabajo, ha sufrido incidentes como**. El encuestado debía seleccionar una o varias respuestas, por tal motivo el nivel porcentual se evalúa sobre los 41 encuestados y no sobre el total de respuestas obtenidas, esto permite alcanzar un porcentaje promedio de riesgo **39.43%,** los cuales afirman haber sufrido algún tipo de eventualidad. Los más frecuentes de mayor a menor se tiene: lentitud en los procesos y discontinuidad en algunos aplicativos o servicios corporativos (internet, aplicaciones, etc.) con un riesgo de 58.54%. Pérdida de conexión con algún aplicativo con riesgo de 51,22%. Seguido de ataques de virus informáticos con riesgo del 43,90%, como se aprecia en el cuadro resumen No 1, estos valores de riesgo, es la causalidad de amenazas que aprovechando la vulnerabilidad del sistema informático si hicieron realidad afectando uno de los pilares de la seguridad informática.

Cuadro No 1: Incidentes informáticos en la estación de trabajo.

10) En su computador de trabajo, ha sufrido incidentes como:	Cantidad	Valor %
a) Ataque de virus informáticos	18	43,90%
b) Perdida de información	7	17,07%
c) Lentitud en los procesos o aplicaciones	24	58,54%
d) Perdida de conexión con algún aplicativo	21	51,22%
e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, etc.	24	58,54%
f) Daño en su equipo de trabajo	3	7,32%
g) Ninguno de los anteriores	6	14,63%

- **Políticas de seguridad informática.** Teniendo en cuenta que la norma ISO NTC- IEC-27001, tienen como objetivo brindar apoyo y orientación a la dirección de la compañía en busca de mayor seguridad de la información, en concordancia con los requisitos del negocio, reglamentos y las leyes pertinentes. En la encuesta a los usuarios de la compañía, se incluyó una pregunta que nos brinda luces sobre el conocimiento de políticas de seguridad Informática, esta es: **4) ¿De los siguientes controles de seguridad informática, cuales aplican en su trabajo?** A la cual responden 39 encuestados que conocen alguna de las políticas de seguridad informática, llamados controles de seguridad informática por la compañía y 2 encuestados no responden la pregunta, como se puede observar en el cuadro No 2, ninguna de las políticas de seguridad informática es aplicada en su trabajo al 100%. Valorando el conocimiento sobre los 41 encuestados, el máximo control de seguridad informática, que es conocido no supera el 80.49% y el mínimo conocimiento es del 23.9%, en promedio los controles son conocidos en un 53.66% del total de las políticas de seguridad informática.

  En el cuadro No. 2, existe una columna a la cual se le dio un valor porcentual a cada control, dependiendo la importancia de la aplicación de la política de seguridad informática, esto se aplica según recomendación del asesor externo de la compañía. Los rangos asignados son del 20%, por ser un control de mayor importancia, 15% a los controles un poco menos importantes y el resto proporcionalmente del 6% y 3%, ya que en su conjunto representan el 50%, obteniendo la gráfica No. 3, que representa una

deficiente aplicabilidad de políticas de seguridad informática en la compañía, la cual llega a un máximo de 58.9% un poco más del promedio 53,66%, para mayor información, anexos 2,3 y 4.

Cuadro No 2: Controles de seguridad informática.

4) ¿De los siguientes controles de seguridad informática, cuales aplican en su trabajo?	Cantidad	Valor % / 41	peso % del control	Resultado
a) Control sobre el uso general del computador en el trabajo,	31	75,61%	3,00%	2,27%
b) Control para el uso de dispositivos de almacenamiento externo (memorias USB)	33	80,49%	3,00%	2,41%
c) Control para el manejo de claves de usuario	33	80,49%	15,00%	12,07%
d) Control para el uso de enlaces Inalámbricos	9	21,95%	6,00%	1,32%
e) Control para el uso del internet www	33	80,49%	3,00%	2,41%
f) Control para realizar copias de seguridad de la información	26	63,41%	20,00%	12,68%
g) Control en el uso del correo electrónico.	26	63,41%	6,00%	3,80%
h) Control para el cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales	26	63,41%	6,00%	3,80%
i) Control sobre el resguardo y protección de la información	23	56,10%	15,00%	8,41%
j) Control para el mantenimiento del computador	18	43,90%	3,00%	1,32%
k) Control para dar de baja un equipo de cómputo o periférico	28	68,29%	4,00%	2,73%
l) Control para modificar o cambiar configuraciones en el computador	10	24,39%	4,00%	0,98%
m) Medidas disciplinarias por incumplimiento de controles informáticos.	23	56,10%	6,00%	3,37%
n) Medidas disciplinarias por incumplimiento de PSI.	9	21,95%	6,00%	1,32%
no sabe no responde	2	4,88%	0,00%	0,00%
TOTAL	5	53.66%	100,00%	58,90%

Teniendo en cuenta el resultado del cuadro No 2, de conocimiento de los controles aplicados en la compañía, se puede obtener la figura No. 2, que permite visualizar el nivel de aplicabilidad catalogados en cuatro niveles a saber: 5%, 10%, 15% y 20%; los cuales fueron obtenidos, aplicando el peso porcentual que se le dio a cada política de seguridad informática, obteniendo un resultado de vulnerabilidad en el conocimiento que tiene cada usuario sobre las políticas de seguridad informática en la compañía.

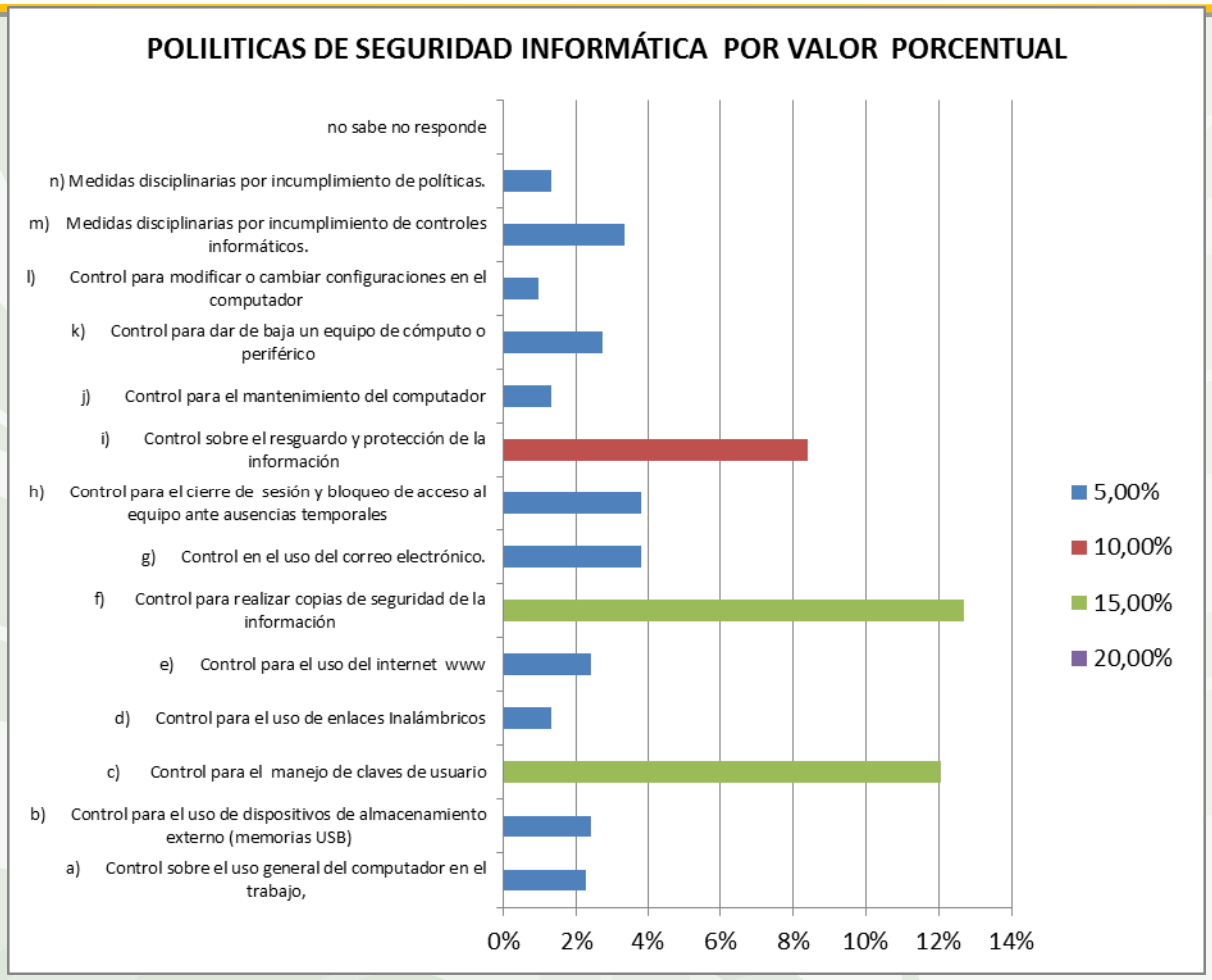


Figura No 2: estadística de conocimiento de Políticas de Seguridad Informática.

Con la gráfica No 3, se pueden apreciar las políticas de seguridad informática, más conocidas por los usuarios del sistema informático en la compañía, por lo cual se da una respuesta a la sub pregunta del proyecto **¿Cuáles son las políticas de seguridad informática definidas y aplicadas actualmente?** Para lo cual se clasifican en cinco (5) niveles de aceptación a saber: insuficiente, no satisfactorio, moderadamente satisfactorio, satisfactorio y totalmente satisfactorio; esto permite visualizar el nivel de conocimiento y aplicabilidad que tiene cada usuario encuestado sobre los controles de seguridad informática aplicados en la compañía y la vulnerabilidad existente.

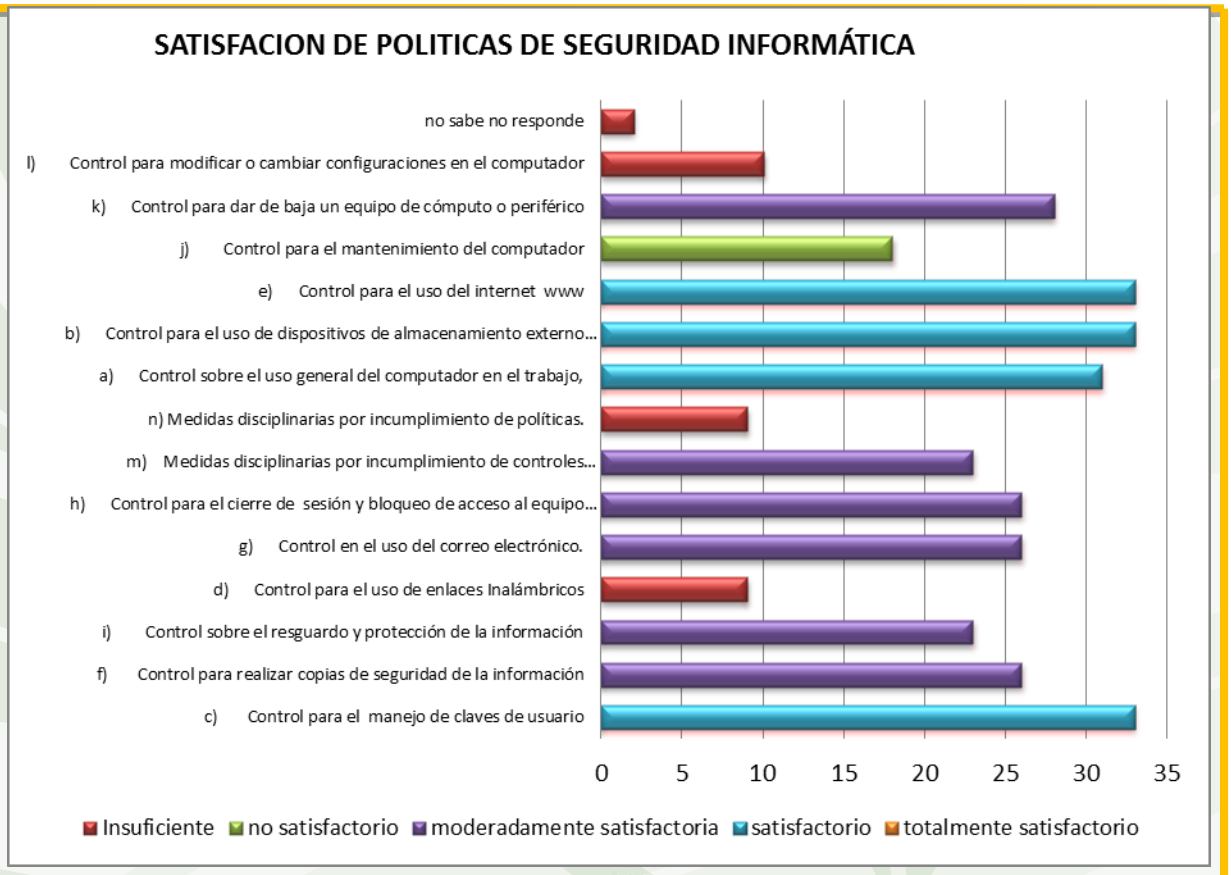


Figura No. 3: Nivel de satisfacción de Políticas de Seguridad Informática.

- **Implementación (Software).** La mayoría del software utilizado en las aplicaciones es realizado a la medida con administración y soporte de terceras personas, uno de los aplicativos importantes que administra y controla la facturación y sistema comercial de la compañía está gestionado por subcontrata (*outsourcing*), los cuales tiene varios recursos humanos (profesionales), que realizan el soporte, la actualización, desarrollo de requerimientos, administración de la aplicación y la base de datos del sistema de información comercial en la compañía, esto tiene sus ventajas y desventajas, entre las desventajas se podría decir que la información se encuentra gestionada y vigilada por terceras personas creando un cierto nivel de dependencia de las personas que no conocen el negocio y por eso no pueden presentar un compromiso y motivación, otra desventaja es que no existe personal calificado que pueda monitorear a la

administración de subcontrata (*outsourcing*), ante esto se podría decir que existen vulnerabilidades y riesgos que amenazan la confiabilidad e integridad de la información en la compañía.

- **Errores de programación.** Existe la posibilidad de presentar errores de programación en las aplicaciones, ya que ningún software de aplicaciones presentes en la compañía se encuentra certificado, como tampoco existen profesionales certificados que avalen estas aplicaciones:
  - Pruebas de Interfaces y Contenidos.
  - Pruebas de Funcionalidades y Operación.
  - Pruebas de Carga.
  - Pruebas de Seguridad informática.
  - Pruebas de Respaldo.

  Tampoco existen herramientas de test de penetración (*pen test* o *penetrationtests*), para verificar la vulnerabilidad de las aplicaciones y sistemas informáticos, estas pruebas requieren un conocimiento sólido y profundo de las tecnologías involucradas en los sistemas, aplicaciones y servicios. Además de una experiencia amplia en el comportamiento de varios sistemas operativos y la complejidad del uso de herramientas; se necesita sagacidad y también pueden representar un gran reto a la inteligencia, para encontrar las vulnerabilidades informáticas y lo más importante corregirlas. Ante esta situación las vulnerabilidades informáticas en las aplicaciones pueden ser inminentes sin que la compañía se percate de ellas.
- **Existencia de puertas traseras,** entre las miles de líneas de código que forman un programa siempre podría haber un fragmento mal diseñado que es imposible prever su comportamiento, y casi siempre se queda sin detectar durante mucho tiempo, pero cuando es descubierto por personas malintencionadas es posible que intente aprovecharlo con fines destructivos; estas puertas traseras o agujeros se presentan en infraestructuras complejas y aplicativos que manejan muchos procesos informáticos, teniendo en cuenta esto, es posible que existan agujeros en los aplicativos de la compañía debido a la complejidad de los mismos, la poca atención

en auditorias que la compañía ha realizado en sus aplicaciones y la utilización de escritorios remotos con *software* libre por los usuarios para procesar información sin autorización del administrador, como lo demuestra la respuesta a la encuesta en la siguiente cuadro No. 3 y que puede representar la existencia de posibles vulnerabilidades informáticas en el sistema operativo y las aplicaciones, para mayor información el anexo No 3 Análisis de la encuesta.

Cuadro No. 3: vulnerabilidad de acceso a escritorio remoto.

DESCRIPCION DE LA RESPUESTA	CANTIDAD	VALOR %
b) Se conecta a través de escritorio remoto al computador de la compañía	6	14,63%
c) Recibe asesoría a través de escritorio remoto	5	12,20%

- **Uso**
  - **Configuración de sistemas informáticos. U**na de las principales herramientas de auditoria de las actividades de los usuarios y los mismos administradores e inclusive para realizar investigación forense en los equipos, cuando existe una eventualidad fraudulenta dentro de los activos de información, es la configuración de los equipos informáticos. Según las entrevistas realizadas a los diferentes administradores estas configuraciones se realizan por los proveedores de los productos informáticos, pero existe ausencia de personal para el monitoreo y vigilancia de estas configuraciones, por este motivo existe una vulnerabilidad que podría ser utilizada por personal interno descontento o inescrupuloso y modificar las configuraciones a beneficio propio.
  - **Desconocimiento de los responsables.** Existe un adagio popular que dice, que la educación es costosa, pero es más costoso el desconocimiento del tema, ante esto se podría decir que la compañía no invierte en capacitar a sus profesionales sobre temas que le permitan desarrollar su trabajo con profesionalismo principalmente en la seguridad informática, muchos empleados que tiene el cargo de profesionales y administradores de sistemas no tienen formación profesional y han adquirido su conocimiento empíricamente, pero desconocen muchas situaciones por la cual

tienen que solicitar la asesoría de terceras personas, que si bien es cierto tienen cláusulas de confidencialidad en sus contratos de prestación de servicios, pueden existir vulnerabilidades con compañías o personas poco comprometidas con la compañía representando un riesgo para los activos de información.

- **Disponibilidad de herramientas.** en el inventario de activos se menciona que no existen herramientas adicionales a las de los sistemas operativos y aplicaciones de la compañía, por este motivo la vulnerabilidad es inminente, ya que no existe un procedimiento o responsable para la utilización de este tipo de herramientas en la compañía.
- **Limitación de tecnologías de seguridad informática.** En la estructura tecnológica de la compañía existen *routers* o *bridges* de varias versiones y marcas, un *firewall* configurado por un especialista certificado, máquinas configuradas como servidores de última versión tecnológica, quienes albergan los activos de información. La administración de algunas áreas de seguridad de la información es responsabilidad de los profesionales de la oficina de planeación y sistemas, en los profesionales de otras oficinas o personal externo. Además, según resultado de las entrevista no existe presupuesto destinado a la modernización y actualización en la seguridad informática, por otro lado la infraestructura jerárquica de recursos humano destinada a la seguridad informática es deficiente, tanto en conocimientos, como en responsabilidades. Ante esto, se podría decir que existe vulnerabilidades tecnológicas en la compañía.

❖ **Hardware.**

- **Control de acceso a los equipos.** De acuerdo al análisis la compañía tiene tres espacios debidamente protegidos con llave física o magnética, para albergar los equipos servidores y de comunicaciones, con ingreso solo de personal debidamente autorizado. Los equipos de cómputo en las estaciones de trabajo de los usuarios internos de la compañía están distribuidos a lo largo y ancho de la edificación en áreas que se pueden asegurar cuando las labores terminan, además cada usuario que ingresa a la compañía se identifica por medio del sistema biométrico, la compañía

que presta el servicio de vigilancia a la compañía no tiene establecido un procedimiento para los visitantes, vulnerabilidad que debe corregirse. En cuanto al acceso lógico se analiza la respuesta que dieron en la encuesta a la pregunta **9) ¿Por labores propias de su desempeño en el trabajo de la compañía ?**, las respuesta son de selección múltiple y se puede concluir que existe vulnerabilidades principalmente en acceso a la información a través de escritorio remoto con aplicaciones gratuitas como fue confirmado en la entrevista a los administradores, estas aplicaciones no brindan ninguna seguridad informática en la transmisión; Los resultados se pueden apreciar en la siguiente cuadro No. 4.

Cuadro No. 4: Vulnerabilidades en la información.

9) ¿Por labores propias de su desempeño en el trabajo de la compañía?	**Cantidad**	**Valor %**
a) Procesa información fuera de la compañía.	10	24,39%
b) Se conecta a través de escritorio remoto al computador de la compañía.	6	14,63%
c) Recibe asesoría a través de escritorio remoto.	5	12,20%
d) No requiere conectarse remotamente.	16	39,02%
e) No requiere llevar información a su casa.	9	21,95%
f) Lo trabaja en horario extendido en la compañía.	23	56,10%
No sabe no responde.	1	2,44%
Total encuestados		**41**

Otra pregunta para verificar la vulnerabilidad de acceso es: **3) ¿Su computador en el trabajo es utilizado por?** En las respuestas se puede observar que el 31.71% es compartido con otras personas estableciendo vulnerabilidades de acceso al sistema de información de la compañía, como se puede evaluar en el siguiente cuadro No. 5:

Cuadro No. 5.Vulnerabilidad de la impericia del usuario.

3) ¿Su computador en el trabajo es utilizado por?	Cantidad	Valor %
a) Solo por usted	28	68,29%
b) Usted y su compañero de confianza	6	14,63%
c) Tres o más personas	3	7,32%
d) Con usuarios invitados o anónimos de vez en cuando.	4	9,76%
Total general	**41**	**100,00%**

- **Control de mantenimiento a los equipos,** revisando la documentación del sistema de gestión de seguridad informática de la compañía existen formatos de cronograma de mantenimiento por sedes y seccionales a los equipos existentes en cada área, donde se especifica el equipo fecha inicial, fecha final y el responsable del equipo, como resultado de las entrevistas los servidores no han recibido ningún tipo de mantenimiento, ya que no existe personal capacitado para este tipo de procedimiento, aunque este tipo de equipos viene construidos para trabajar sin interrupciones los 365 días al año, podría existir vulnerabilidad con amenaza de daño en el servidor por falta de mantenimiento.

❖ **Usuarios.**

- **Hábitos de acceso a los equipos y el nivel de conocimiento sobre seguridad informática.** Para el desarrollo del ítem se realizó encuestas cuyo análisis y resultado se encentran en el anexo 2 y 3.

4.3.2. Amenazas informáticas.

Una amenaza informática es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño material o inmaterial sobre los sistemas informáticos, vulnerando uno de los pilares de la Seguridad Informática como son: la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

❖ **Amenaza del Entorno (seguridad física**). Sucesos o eventos que pueden ocurrir con o sin intervención de los seres humanos, causando daño a los equipos informáticos

(hardware), soporte de información, equipamiento auxiliar, instalaciones, medios de comunicación, etc. Estas amenazas se encuentran presentes en:

- **Daño por fuego (Incendio).** La posibilidad de que el fuego acabe con los recursos de información del sistema, los cuales pueden ser causados por diferentes aspectos como lo son las personas que fuman, por un corto circuito en las instalaciones eléctricas de la edificación o por vandalismo debido a su cercanía con la calle, también puede ser ocasionados por falla en la ventilación o aire acondicionado lo que causaría un aumento de temperatura en los equipos servidores.
- **Daños por agua**. Escapes, fugas, inundaciones; son posibilidades de que el agua acabe con los recursos del sistema de información, estos daños pueden ser causados por un deterioro en la tubería de agua presente en la edificación, también existe otro riesgo inminente debido a la cercanía de los cuartos de servidores a una fuente hídrica, perteneciente al espacio de la compañía.
- **Desastres Naturales como**. Incidentes que se producen por: tormentas eléctricas, ciclones, avalanchas, deterioro de suelos, contaminación, siniestro mayor, fenómenos (climático, sísmico, de origen volcánico, meteorológico e inundación), el de origen volcánico es de mayor riesgo por encontrarse en una ciudad cercana a un volcán activo.
- **Daños de origen Industrial.** Daños que pueden ocurrir de forma accidental por el entorno o deliberada por la actividad humana, la amenazas como de origen industrial (fuego, daños por agua); desastres industriales (explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico) Contaminación mecánica (vibraciones, polvo suciedad); Contaminación electromagnética (interferencias de radio, campos o impulsos electromagnéticos).
- **Avería de origen físico o lógico.** Fallos en los equipos y/o en los programas, puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema y muy difícil de saber si es de origen físico o lógico por deterioro del *hardware* o fallas en su funcionamiento, esto puede ocurrir por falta de

mantenimiento en los equipos de cómputo o por manejo inadecuado de memorias USB las cuales pueden estar infectadas de virus informáticos

- **Fallo de servicios de comunicaciones.** Se debe a la destrucción física de los medios físicos de transporte o a los centros de conmutación, por pérdida del suministro de energía, condiciones inadecuadas de temperatura o humedad, fallas en la climatización como excesivo calor, frio, humedad, etc. Según el resultado de la encuesta estos incidentes se presentan con frecuencia, un 58% de los encuestados afirman haber sufrido de fallas en la comunicación y disponibilidad de la información.

- **Negligencia y decisiones institucionales.** Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema con responsabilidades de instalación y operación, también con deficiencias organizativas cuando no está claro quien tiene que hacer exactamente qué, existen acciones descoordinadas errores por omisión y cuándo incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionadas con el comportamiento humano afectando la integridad, confidencialidad y disponibilidad de los activos de información como datos y/o información, claves criptográficas, servicios, aplicaciones, soportes de información, equipos informáticos, redes de comunicación, entre otros, por amenazas como:
  - Programas no autorizados / software pirateado. Falta de pruebas de software nuevo con datos productivos. Infección de sistemas a través de unidades portables sin escaneo. Mal manejo de sistemas y herramientas, Falta de inducción, capacitación y sensibilización sobre riesgos. Manejo inadecuado de datos críticos (codificar, borrar, etc.). Dependencia a servicio técnico externo. Perdida de datos. Unidades portables con información sin cifrado. Transmisión no cifrada de datos críticos. Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada). Compartir contraseñas o permisos a terceros no autorizados,

Transmisión de contraseñas por teléfono. Exposición o extravío de equipo, unidades de almacenamiento, etc. Sobrepasar autoridades. Falta de definición de perfil, privilegios y restricciones del personal. Falta de mantenimiento físico (proceso, repuestos e insumos). Falta de actualización de software (proceso y recursos). Fallas en permisos de usuarios (acceso a archivos). Acceso electrónico no autorizado a sistemas externos. Acceso electrónico no autorizado a sistemas internos. Red cableada expuesta para el acceso no autorizado. Red inalámbrica expuesta al acceso no autorizado. Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos). Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control. Ausencia de documentación.

- **Amenazas de criminalidad (común y política). S**on todas las acciones, causadas por la intervención humana, que violan la ley y políticas de seguridad informática de la compañía en busca de un beneficio propio o simplemente con el ánimo de causar daño a los activos de la compañía. La criminalidad política de seguridad informática se entiende como todas las acciones dirigidas desde el gobierno hacia la sociedad civil. Por ser acciones del recurso humano, son una de las amenazas más difíciles de controlar y que se presentan al interior y/o exterior de la compañía, por razones como: empleados descontentos, empleados cleptómanos, ex empleados disgustados, intrusos, etc.; los cuales pueden tener alto conocimiento tecnológico e información sensible de la compañía y se crea la necesidad de diversión o lucro personal y que aprovechando los fallos en la red o equipos informáticos ven la oportunidad de causar daños en los activos de información de la compañía con acciones como: la manipulación de la configuración, modificación deliberada de información, manipulación de programas los cuales pueden desviar información, robo de información o fondos de la compañía, acceso no autorizado, extorsión, ingeniería social. Las amenazas que clasifican como criminales son:
  - Allanamiento (ilegal, legal).
  - Persecución (civil, fiscal, penal).
  - Orden de secuestro / Detención.

- Sabotaje (ataque físico y electrónico).
- Daños por vandalismo.
- Extorsión.
- Fraude / Estafa.
- Robo / Hurto (físico).
- Robo / Hurto de información electrónica.
- Intrusión a Red interna.
- Infiltración.
- Virus / Ejecución no autorizado de programas.
- Violación a derechos de autor.

4.3.3. Riesgos informáticos

El riesgo informático se puede definir como aquel incidente que imposibilita el cumplimiento de un objetivo. En informática el riesgo se plantea como el producto de la magnitud de un daño en un activo por la probabilidad de ocurrencia de una amenaza, aprovechando las vulnerabilidades existentes en el sistema. Para determinar los riesgos informático en la compañía se tiene en cuenta lo mencionado en el apartado de activos de información, los cuales son valorados de acuerdo a la magnitud del daño en la compañía de la siguiente manera:

- 1 = Insignificante, valor es muy pequeño, poco importante o que carece de valor
- 2 = Bajo, daño menor
- 3 = Medio, daño importante
- 4 = Alto, daño grave y/o muy grave

De igual manera se dio el mismo valor para la probabilidad de ocurrencia de las amenazas, las cuales fueron enunciadas en párrafos anteriores, con los activos encontrados en la compañía y las amenazas expuestas, se construye la matriz de riesgos informáticos en base a la valoración de la cuadro No. 6.

Cuadro No. 6 matriz de riesgos informáticos.

En la cuadro anterior se asigna tres colores para asignar el grado de daño causado a los activos de información como se observa en la cuadro No. 7.

Cuadro No. 7: Valor del riesgo informático

RIESGO	VALOR	DAÑO CAUSADO	SIGNIFICADO DEL COLOR
BAJO RIESGO	(1 A 6)	DAÑO MENOR EN EL ACTIVO	SEÑAL DE SEGURIDAD INFORMÁTICA
MEDIO RIESGO	6.1 a 9	DAÑO IMPORTANTE EN ELACTIVO	SEÑAL DE ATENCION
ALTO RIESGO	9,1 a 16	DAÑO GRAVE Y/O EXTREMADAMENTE GRAVE	SEÑAL DE PELIGRO ATENCION INMEDIATA

Para la elaboración del mapa de riesgos informáticos, se tiene en cuenta cada uno de los factores de riesgo informático enunciados en el párrafo de amenazas, a los cuales se les asigna un valor de probabilidad de ocurrencia por un valor de magnitud del daño causado a los activos identificados en el desarrollo del primer objetivo, teniendo en cuenta el análisis de las encuestas y entrevistas realizadas en la compañía (mayor información ver anexos 1, 2 y 3), por efectos prácticos, para al final tener una idea global del resultado del mapa de riesgos se realizan tres grupos de amenazas informáticas como son:

- Actos originados por la criminalidad común y motivación política
- Sucesos de origen físico.
- Sucesos derivados de la negligencia de usuarios/as y decisiones institucionales.

❖ Los activos se agruparon de la siguiente manera:

- Incidentes en Datos e Información.
- Incidentes en la Infraestructura de Sistemas.

- Incidentes con el Personal.

Teniendo en cuenta el grupo de amenazas informáticas y activos de información mencionados en el apartado anterior, se inicia el análisis de riesgos teniendo en cuenta cada uno de los factores de que se vislumbran en cada grupo.

- **Actos originados por la criminalidad común y motivación política:**
  - Para ello se contemplan los siguientes: Allanamiento (ilegal, legal); Persecución (civil, fiscal, penal); Orden de secuestro / Detención; Sabotaje (ataque físico y electrónico); Daños por vandalismo; Extorsión, Fraude / Estafa, Robo / Hurto (físico); Intrusión a Red interna; Infiltración; Virus / Ejecución no autorizado de programas; Violación a derechos de autor.
- **Sucesos de origen físico.**
  - En los sucesos de origen físico se distinguen los siguientes amenazas: Allanamiento (ilegal, legal); Persecución (civil, fiscal, penal); Orden de secuestro / Detención, Sabotaje (ataque físico y electrónico); Daños por vandalismo; Extorsión, Fraude / Estafa Robo / Hurto (físico); Robo / Hurto de información electrónica; Intrusión a Red interna; Infiltración; Virus / Ejecución no autorizado de programas y Violación a derechos de autor.
- **Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.**
  - Incendio. Inundación / decolore, Sismo, Polvo. Falta de ventilación, Electromagnetismo. Sobrecarga eléctrica; Falla de corriente (apagones). Falla de sistema / Daño disco duro. Falta de inducción, capacitación y sensibilización sobre riesgos. Mal manejo de sistemas y herramientas. Utilización de programas no autorizados / software 'pirateado. Falta de pruebas de software nuevo con datos productivos. Perdida de datos Infección de sistemas a través de unidades portables sin escaneo. Manejo inadecuado de datos críticos (codificar, borrar, etc.). Unidades portables con información sin cifrado. Transmisión no cifrada de datos críticos. Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada). Compartir contraseñas o permisos a terceros no autorizados.

Transmisión de contraseñas por teléfono. Exposición o extravío de equipos, unidades de almacenamiento, etc. Sobrepasar autoridades. Falta de definición de perfil, privilegios y restricciones del personal. Falta de mantenimiento físico (proceso, repuestos e insumos). Falta de actualización de software (proceso y recursos). Fallas en permisos de usuarios (acceso a archivos). Acceso electrónico no autorizado a sistemas externos. Acceso electrónico no autorizado a sistemas internos. Red cableada expuesta para el acceso no autorizado. Red inalámbrica expuesta al acceso no autorizado. Dependencia a servicio técnico externo. Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos). Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control y Ausencia de documentación de seguridad informática.

Lo más importante en la compañía de **PROPOLSINECOR** son los activos de información que para efecto de análisis se clasificó en tres grupos que se mencionaron en apartados anteriores y para encontrar la magnitud del daño de cada activo se relaciona a continuación:

4.3.4. Magnitud de daño en datos e información.

Los activos pertenecientes a este grupo se observa en la cuadro No. 8, Matriz de análisis de riesgo a datos e información; los resultados son sorprendentes y algunos de los activos se encuentran en alto riesgo y sobrepasan el 50% , por tal motivo se crearan PSI que permitan mitigar el riesgo y salvaguardar los activos en alto riesgo informático.

Cuadro No 8. Matriz de análisis de riesgo a datos e información

Valoración de los activos y amenazas		Valores de magnitud de Daño: [1 = Insignificante, 2 = Bajo, 3 = Mediano, 4 = Alto]								
		Valores probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]								
Matriz de Análisis de Riesgo		Probabilidad de Amenaza								
Datos e Información	Magnitud de daño	Actos originados por la criminalidad común y motivación política			Sucesos de origen físico			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		
		RIESGO								
	valor	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
Información financiera	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Servicios bancarios	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Información comercial	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Información técnica y especifica de la compañía	3	62%	38%	0%	89%	11%	0%	42%	46%	15%
Directorio de Contactos	3	62%	38%	0%	89%	11%	0%	42%	46%	15%
información de seguimiento a metas	3	62%	38%	0%	89%	11%	0%	42%	46%	15%
Administración documental	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Información del sistema de gestión de seguridad informática	3	62%	38%	0%	89%	11%	0%	42%	46%	15%
Información de administración y configuración de las comunicaciones	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Base de datos para procesar información financiera y administrativa	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Base de datos de información comercial	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Base de datos documentales	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Código ejecutable (aplicaciones)	3	62%	38%	0%	89%	11%	0%	42%	46%	15%
Datos de prueba	2	100%	0%	0%	100%	0%	0%	88%	12%	0%

Cuadro No 8 (Continuación) Matriz de análisis de riesgo a datos e información

Valoración. de los activos y amenazas		Valores de magnitud de Daño: [1 = Insignificante, 2 = Bajo, 3 = Mediano, 4 = Alto]								
		Valores probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]								
Matriz de Análisis de Riesgo		Probabilidad de Amenaza								
Datos e Información	Magnitud de daño	Actos originados por la criminalidad común y motivación política			Sucesos de origen físico			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		
		RIESGO								
	valor	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
Herramientas de navegación Internet	2	100%	0%	0%	100%	0%	0%	88%	12%	0%
Claves criptográficas	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Correo electrónico	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Almacenamiento de ficheros	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Gestión de Privilegios	4	15%	46%	38%	44%	44%	11%	0%	42%	58%
Promedio datos e Información		**34%**	**41%**	**25%**	**61%**	**32%**	**7%**	**18%**	**41%**	**42%**

4.3.5. Magnitud de daño en sistema e infraestructura.

Los activos informáticos pertenecientes a este grupo se observa en la cuadro No 13 Matriz de análisis de riesgo sistema e infraestructura; los resultados de alto riesgo llegan a un 62% lo que implica tomar medidas correctivas

Cuadro No. 9 Matriz de análisis de riesgo de sistemas e infraestructura:

Valoración de los activos y amenazas	Valores de magnitud de Daño: [1 = Insignificante, 2 = Bajo, 3 = Mediano, 4 = Alto]									
	Valores probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]									
Matriz de Análisis de Riesgo		Probabilidad de Amenaza								
Sistemas e Infraestructura	Magnitud de daño	Actos originados por la criminalidad común y motivación política			Sucesos de origen físico			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		
		RIESGO								
	valor	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
Equipos de la red cableada (*router*, *switch*, etc.)	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Equipos de la red inalámbrica (*router*, punto de acceso, etc.)	3	38%	54%	8%	78%	22%	0%	38%	54%	8%
Cortafuego	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Servidores de gestión	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Computadoras de escritorio	2	92%	8%	0%	100%	0%	0%	92%	8%	0%
Portátiles	3	38%	54%	8%	78%	22%	0%	38%	54%	8%
Programas de administración (contabilidad, manejo de personal, etc.)	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Programas de manejo de proyectos	3	38%	54%	8%	78%	22%	0%	38%	54%	8%
Programas de producción de datos (facturación y otros)	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	3	38%	54%	8%	78%	22%	0%	38%	54%	8%
Impresoras	2	92%	8%	0%	100%	0%	0%	92%	8%	0%
Memorias portátiles	4	31%	8%	62%	33%	44%	22%	0%	38%	62%
Dispositivos de frontera	3	38%	54%	8%	78%	22%	0%	38%	54%	8%
Respaldo eléctrico	2	92%	8%	0%	100%	0%	0%	92%	8%	0%
Infraestructura eléctrica	2	92%	8%	0%	100%	0%	0%	92%	8%	0%
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	2	92%	8%	0%	100%	0%	0%	92%	8%	0%
Promedio Sistemas e Infraestructura		52%	22%	25%	68%	24%	8%	41%	34%	25%

4.3.6. Magnitud de daño Personal.

Los activos pertenecientes a este grupo son impredecibles debido a que intervienen la actividad humana como se observa en la cuadro No 10 Matriz de análisis de riesgo de personal; los resultados de alto riesgo llegan a un 62% lo que implica tomar medidas correctivas, y crear PSI.

Cuadro No. 10 Matriz de análisis de riesgo de sistemas e infraestructura:

Valoración de los activos y amenazas		Valores de magnitud de Daño: [1 = Insignificante, 2 = Bajo, 3 = Mediano, 4 = Alto] Valores probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]								
Matriz de Análisis de Riesgo		Probabilidad de Amenaza								
Personal	Magnitud de daño	Actos originados por la criminalidad común y motivación política			Sucesos de origen físico			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		
		RIESGO								
	valor	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
Junta Directiva	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Dirección / Coordinación	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Administradores de BBDD y Aplicativos	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Administración	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Personal técnico	2	85%	15%	0%	100%	0%	0%	92%	8%	0%
subcontratas (*outsourcing*)	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Recepción	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Piloto / conductor	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Informática / Soporte técnico interno	3	69%	15%	15%	78%	22%	0%	38%	54%	8%
Soporte técnico externo	4	54%	15%	31%	67%	11%	22%	0%	38%	62%
Servicio de limpieza de planta	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Servicio de limpieza externo	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Servicio de mensajería de propio	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Servicio de mensajería de externo	1	100%	0%	0%	100%	0%	0%	100%	0%	0%
Promedio Personal		77%	9%	14%	84%	6%	10%	52%	21%	27%

Analizado los riesgos informáticos del cuadro macro y resumiendo en grupos los activos como ya se había mencionado. Teniendo en cuenta el valor del activo de acuerdo a la magnitud del daño causado por una probabilidad de ocurrencia de una amenaza, se obtiene resultados promedio como se observa en la cuadro No 11 Análisis de riesgo promedio, como resultado se puede observar, que existe riesgos de alto impacto (rojo) los cuales pueden causar daño a los activos de datos e información, por amenazas de negligencia institucional y los riesgos de impacto medio (color amarillo) que pueden causar daño a los activos de datos e información y sistemas e infraestructura por criminalidad común o política y a los activos sistemas e infraestructura y personal por negligencia institucional.

Cuadro No. 11: Análisis de riesgos promedio.

Análisis de Riesgo promedio		Probabilidad de Amenaza		
		Criminalidad común	Sucesos de origen físico	Negligencia Institucional
Magnitud de Daño	Datos e Información	8.0	6.0	9.8
	Sistemas e Infraestructura	7.3	5.8	8.2
	Personal	4.6	3.9	6.7

Siguiendo con el análisis se computa porcentualmente cada probabilidad de ocurrencia lo cual se observa en la cuadro No 12.

Cuadro No. 12: Análisis de riesgo porcentual por niveles

Análisis de Riesgo porcentual por Niveles		Probabilidad de Amenaza								
		Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
		Actos originados por la criminalidad común y motivación política			Sucesos de origen físico			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales		
Magnitud de Daño	Datos e Información	34.0%	40.8%	25.2%	60.5%	32.2%	7.3%	17.8%	41.2%	42.0%
	Sistemas e Infraestructura	52.4%	22.1%	25.5%	68.1%	23.6%	8.3%	40.9%	33.7%	25.5%
	Personal	76.9%	8.8%	14.3%	84.1%	6.3%	9.5%	52.2%	20.9%	26.9%

Exponiendo un poco más detallado el análisis promedio de riesgo por cada uno de grupo de activos evaluados se obtiene resultados de alto riesgo informáticos, que llegan a un

porcentaje de 62%, lo que implica tomar medidas correctivas para los de alto impacto y montar buenas practicas con el ánimo de salvaguardar los activos de información de la compañía de un eventual daño.

Graficando cada grupo de amenazas informáticos, existen riesgos informáticos de alto cuidado como se observa en las siguientes figuras No. 4, No. 6 y No. 7

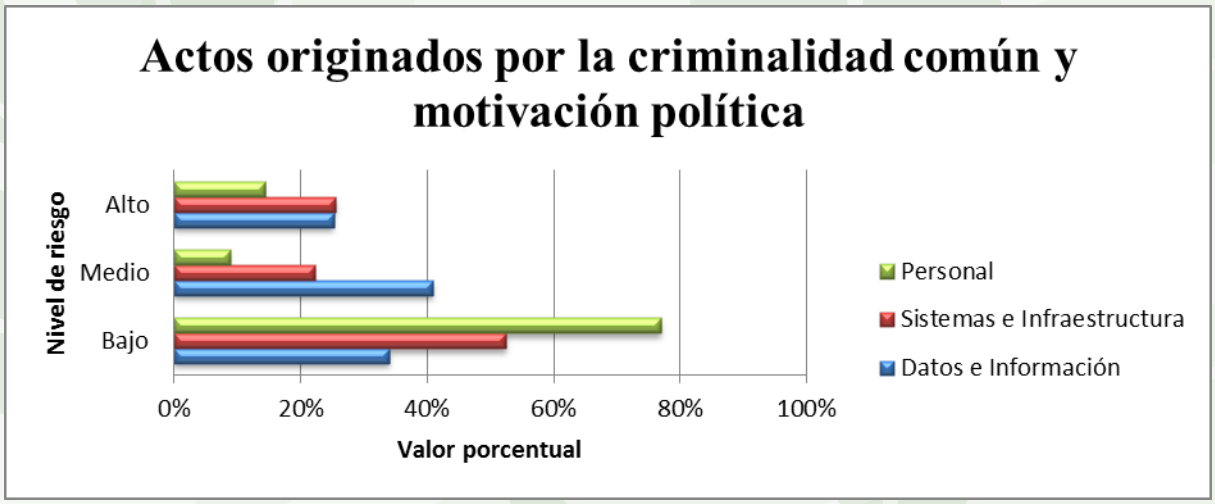


Figura No. 4: Criminalidad común y política.

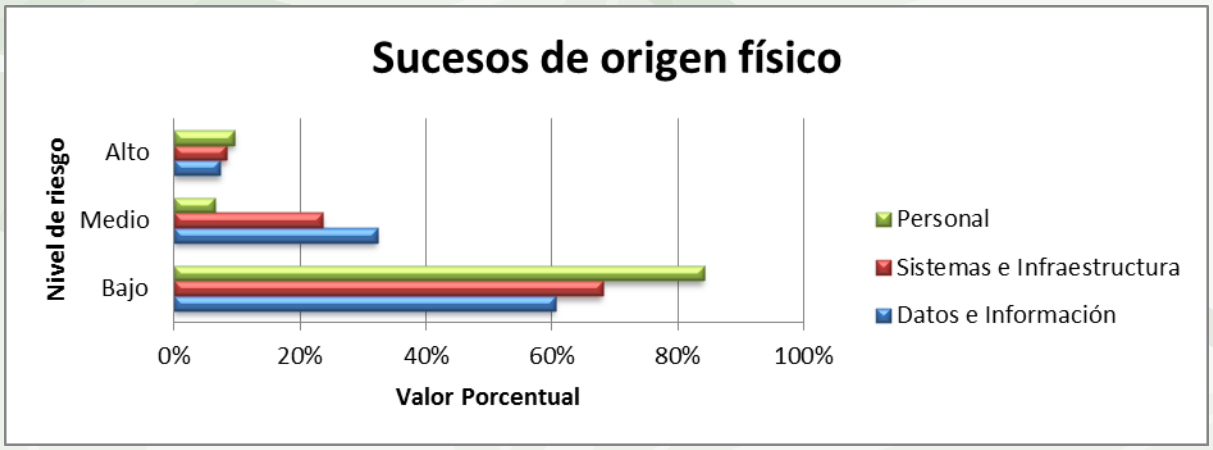


Figura No 5: Origen físico.

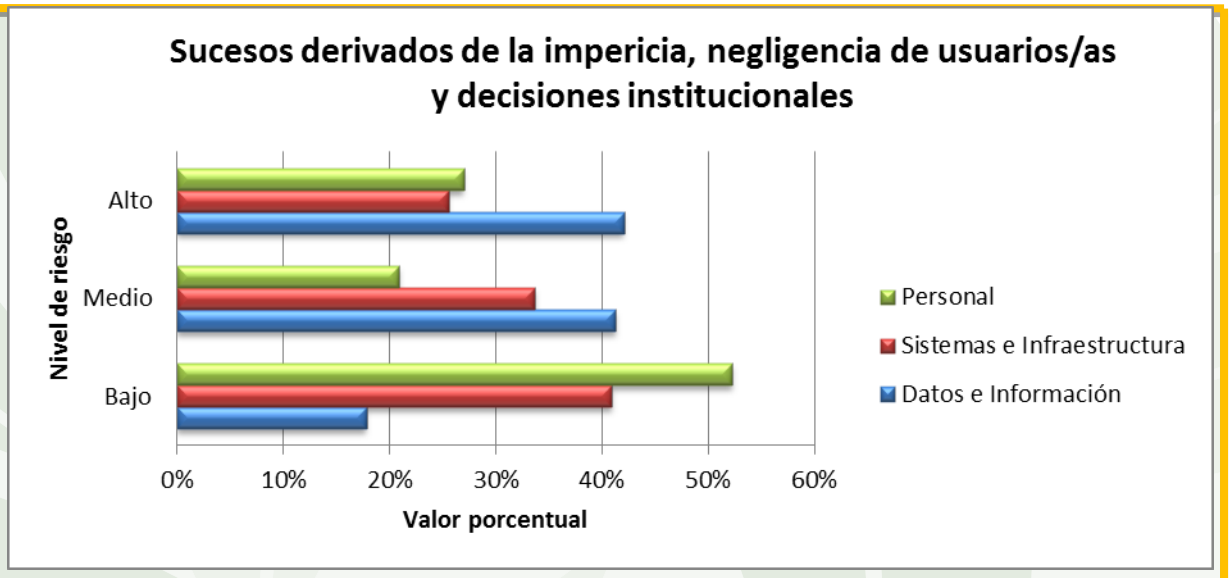


Figura No. 6: Impericia y negligencia administrativa.

En conclusión los riesgos de algunos activos informáticos son altos, por tanto se debe tomar correctivos de implementar salvaguardas que permitan minimizar el riesgo al cual están expuestos los activos informáticos de la compañía.

4.4. VALORACION DE LOS ESTÁNDARES EN LA SEGURIDAD INFORMÁTICA IMPLEMENTADOS EN LA COMPAÑÍA

De acuerdo al desarrollo de cada objetivo de este proyecto se ha podido apreciar que existen políticas de seguridad informática y no se encuentran totalmente difundidas a todo el personal de la compañía, en cuanto a los estándares se analizó la documentación (ver anexo 1) y se puede expresar que se aplican algunos apartes de los controles de la norma ISO 27001 y norma ISO 27002 como parte del documento Sistema de Gestión de Seguridad de la Información contempla.

4.4.1. La Infraestructura de la Seguridad de la Información vislumbra lo siguiente.

- Comité de la seguridad de la información está constituido por directivos de la compañía, los cuales se reúnen regularmente para discutir necesidades de ampliación e

implementación de nuevas tecnologías e incidentes presentados, y las posibles soluciones.

- Tiene identificado los sistemas de información más sensibles de la compañía y asignado responsabilidad del proceso a una oficina específica, pero existen activos muy sensibles asignada la operación y el mantenimiento a un tercero (*outsourcing*), Además les falta inventariar cada activo informático existente, dejándolo debidamente identificado, rotulado y clasificado en una base de datos con responsabilidades específicas.
- Tiene contemplado políticas de seguridad informática frente al acceso por parte de terceros, pero le falta el control y monitoreo de acceso de la tercerización de procesos por falta de personal calificado para este tipo de labores, como también se debe contemplar la capacitación, concientización de los riesgos, sus responsabilidades son adecuados para los roles para los que se los considera, y reducir el riesgo de otro fraude o uso inadecuado de las instalaciones.

4.4.2. Actos originados por la criminalidad común y motivación política.

- Tiene implementadas PSI de respuesta a incidentes y anomalías del *software* en materia de seguridad informática, algunas de las nombradas son contempladas pero otras las pasan por alto.

4.4.3. Seguridad física y ambiental.

- **A**nte esto tiene documentado y contemplado las siguientes PSI:
  - **Perímetro de seguridad física**. Controles de acceso físico, protección de oficinas recintos e instalaciones, desarrollo de tareas en áreas protegidas.
  - **Ubicación y protección del equipamiento de copias de seguridad informática.** Se encuentran documentadas e implementadas en la compañía, pero no se difunden a todos los usuarios y no se realiza seguimientos de control.
  - **Suministro de energía**, Para ello tiene implementado respaldo limitado con *UPS*, pero le falta la implementación de circuitos redundantes en caso de ausencias de energía prologados.

- **También contempla PSI como seguridad informática del cableado**. Mantenimiento y seguridad informática de los equipos fuera de las instalaciones, desafectación o reutilización segura de equipos, PSI de escritorios, pantallas limpias y retiro de los bienes; ante esto se diría que falta contemplar la política de eliminación o sanitización de equipos de cómputo.

4.4.4. Gestión de comunicaciones y operaciones.

Se podría decir que se encuentra documentado cada control como la norma lo exige como: los procedimientos operacionales y responsabilidades; planificación y aceptación de sistemas; protección contra *software* malicioso; mantenimiento; Administración y seguridad de los medios; Intercambio de información y *software*; realizando la comparación falta algunos controles que afirmarían la seguridad del sistema informático los cuales se tendrán en cuenta en la elaboración de políticas de seguridad informática.

4.4.5. Control de accesos.

En ellos se contempla requerimientos para el control de acceso; administración de acceso de usuarios; responsabilidad del usuarios; control de acceso a la red, al sistema operativo, a las aplicaciones, computación móvil y trabajo remoto; este objetivo lo tiene implementado en su totalidad de acuerdo a la norma, pero para muchos controles de acceso no se cumple en un ciento por ciento por falta de divulgación y conocimiento de los usuarios como en la configuración de los sistemas y aplicaciones.

4.4.6. Desarrollo y mantenimiento de los sistemas.

En este objetivo contemplan los siguientes controles como son: requerimiento de seguridad informática de los sistemas, aplicaciones, controles criptográficos, seguridad informática de archivos del sistema, seguridad informática de procesos de desarrollo y soporte, como parte de este objetivo no contemplan Gestión de vulnerabilidad técnica, como lo contempla la norma. Además, muchos controles enunciados por la compañía no se encuentran implementados como los criptográficos y los otros controles se encuentran implementados

en algunos activos informáticos y no manejan un estándar para todas las aplicaciones de la compañía como tampoco el manejo de archivos del sistema informático.

4.4.7. Gestión de los incidentes de la seguridad de la información.

Este objetivo no lo tiene documentado o implementado la compañía no cumpliría con el estándar de la norma.

4.5. PLAN DE SENSIBILIZACIÓN, DIFUSIÓN Y CAPACITACIÓN EN POLÍTICAS DE SEGURIDAD INFORMÁTICA.

La campaña de sensibilización está enfocada principalmente en dar a conocer los riesgos a los que pueden estar expuestos los sistemas de información, los usuarios, las redes y la información en general, las amenazas internas y externas por violentar el cumplimiento de buenas prácticas respecto a la seguridad de la información, estás buenas prácticas actúan de manera preventiva ayudando a la compañía a salvaguardar sus activos de información.

El plan de sensibilización difusión y capacitación de las políticas de seguridad informática (PSI), es parte indispensable dentro de cualquier programa de Gestión de Seguridad Informática que se quiera implementar en una compañía, por el hecho de requerir que todos y cada uno de los que conforman la compañía, formen parte de este esfuerzo conjunto, para la generación de un buen nivel de seguridad informática, el cual trae consigo ventajas para el mejor aprovechamiento de los recursos informáticos, de la misma forma para evitar diversos tipos de incidentes.

Las políticas de seguridad informática (PSI) establecen lo que se debe o necesita hacer para la seguridad informática y porque, explicando la importancia de los lineamientos contenidos en la política de seguridad informática, que pueden ser vistos por todo el personal de la compañía sin importar el cargo que desempeñe dentro de ella, para ello deberá ser informado de la importancia del cumplimiento de la política de seguridad informática, que se implementa en la compañía. De esta forma se hará conciencia de la importancia de su participación y colaboración en todo el proceso de desarrollo logrando

conseguir que todos los usuarios que integran la compañía sean conscientes de los riesgos de los sistemas de Gestión de Seguridad de la Información.

Crear una cultura en donde todos los miembros de la compañía comprendan la importancia de dar un tratamiento adecuado a la información en pro de integridad, confidencialidad y disponibilidad de la información, es el resultado de una eficiente participación y capacitación adecuada de todo el personal que conforma la compañía, de esta manera cada usuario o individuo entenderá la importancia de la información que le fue confiada para la realización de su trabajo así como la propia, estas capacitaciones estará directamente relacionada con el nivel de seguridad informática , es decir entre mayor capacitación del personal haya el nivel se seguridad de la información será mucho más alto como se describe en la cuadro No 13.

Cuadro No. 13: Capacitación.

BUENA	MALA	ERRONEA
Bien capacitado tiene una cultura y clara idea de lo importante que es la información para la compañía. Sabe cómo proteger los activos de información o bienes tanto propios como los que la compañía confía en él	Está expuesto a un posible incidente por desconocimiento y no tener una buena capacitación. Propensión a cometer errores que pueden facilitar la perdida destrucción mal uso de la información o el facilitar un incidente	Actúa con temor ante cualquier tipo de actividad con la idea de que todo el mundo es un posible agresor que busca robar o destruir su información.

4.5.1. Plan de difusión y sensibilización de las políticas de seguridad informática.

Una vez creadas las políticas de seguridad informática (se presentan en el capítulo siguiente) es muy importante establecer una estrategia de difusión y sensibilización sobre las mismas. En el cuadro 14 se presenta el plan de difusión y sensibilización, pero no contemplan el cronograma debido a que la propuesta debe ser aprobada y aceptada por la compañía antes de fijarse los tiempos.

Cuadro No. 14: Difusión y sensibilización de políticas de seguridad informática.

ATIVIDAD	PROPOSITO	RESPONSABLE	RECURSOS
1.0 Crear cronograma de difusión y sensibilización	Que el usuario este actualizado y concientizado de la aplicación de las PSI	Dirección de Planeación y sistemas	Políticas de seguridad informática
2.0 Reproducción de PSI	Que todos el personal tenga y conozca las PSI	Dirección de Planeación y sistemas	Económicos
3.0 Creación de cartillas didácticas de PSI	Que los usuarios conozcan de manera didáctica las PSI	Dirección de Planeación y sistemas y áreas de difusión	Económicos, publicidad
4.0 Difusión por medio de intranet	Entrega por correo videos, cartillas didácticas con los aspectos más relevantes de las PSI	Dirección de planeación y sistemas	Tiempo y medios electrónicos
5.0 capacitación de formación presencial	Sensibilizar y concientizar a los usuarios de la importancia de aplicar las PSI	Dirección de Planeación y Sistemas Usuarios del Sistema	Auditorio, Computador, expositor y logística de capacitación
6.0 Taller de formación personal	Sensibilizar y concientizar a los usuarios de los riesgos por incumplimiento de PSI	Dirección de Planeación y Sistemas Usuarios del Sistema	Auditorio, Computador, expositor y logística de capacitación
7.0 Charlas, campañas, conferencias y seminarios	Que los directivos se concienticen y sensibilicen de aplicar las PSI.	Dirección de Planeación y Sistemas Directivos	Auditorio, Computador, expositor
8.0 Carteles en los espacios de publicación y anuncio de la compañía	Educar de forma didáctica del riesgo de incumplir las PSI	Dirección de Planeación y Sistemas Todos	Cartelera y publicidad

Para que la sensibilización y concientización de las PSI sean efectivas, la compañía debe utilizar la publicidad para su divulgación y difusión por diversos medios como: páginas web, correo electrónico, carteles dentro de la misma compañía, etc; para ello es importante que las políticas de seguridad informática estén redactadas en forma didáctica para llegar a todos los usuarios tanto internos como externos; un ejemplo de este tipo de carteles o publicidad se muestra en la gráfica No. 7, en la cual se hace mención a una serie de fallas que se pueden evitar, para ello el área encargada de la oficina de Planeación y Sistemas con un experto en publicidad, debe crear las diapositivas de divulgación, esto permitirá llegar y crear cultura en los usuarios de la compañía.

Figura No. 7: Publicación de políticas de seguridad informática en cartelera,

Fuente: Difusión de PSI de seguridad Informática www.ingeniería.unam.mx/psc-fi.html.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Estas políticas tiene como propósito proteger la información de las amenazas, a fin de garantizar la continuidad de los sistemas de información, con la documentación de los activos que permita mitigar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Compañía.

Es importante que los principios de la política de seguridad informática sean parte de la cultura Empresarial, para esto se manifiesta un compromiso de parte de las máximas Autoridades de Compañía y de los titulares de diferentes áreas Empresariales para la difusión, consolidación y cumplimiento de la presente política de seguridad informática.

5.1. OBJETIVOS

a) Proteger los recursos de los sistemas de información de la Compañía y la tecnología utilizada para su procesamiento, frente a amenazas a la seguridad informática internas o externas, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Adecuar la implementación de las medidas de seguridad informática comprendidas en la Política, identificando los recursos y las reservas presupuestales correspondientes, contando con el apoyo de la Dirección, alineada con las estrategias y objetivos de la compañía.

c) Mantener las políticas de seguridad informática de la compañía actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

5.2. RESPONSABILIDAD

Todos los directivos y demás personal, sea cual fuere su nivel jerárquico serán responsables de la aplicación de estas políticas de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha PSI por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal involucrado en los Sistemas de Información de la Compañía, cualquiera que sea su situación contractual y el Gerente General de la Compañía apruebe estas PSI y las modificaciones que sean necesarias.

5.3. CUMPLIMIENTO

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad informática.

A fin de asegurar la implementación de las medidas de seguridad de la información comprendidas en esta políticas de seguridad informática, la compañía identificará los recursos necesarios e indicará formalmente las reservas presupuestales correspondientes, como anexo a la presentes políticas de seguridad informática. Lo expresado anteriormente no implicará necesariamente la asignación de partidas o reservas adicionales.

El Comité de Seguridad de la Información revisará semestralmente las presentes políticas de seguridad informática, a efectos de mantenerla actualizada. Así mismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad informática, etc.

5.4. SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de las disposiciones establecidas en las políticas de seguridad de la información, tendrá como resultado la aplicación de diversas sanciones conforme a la magnitud y característica del aspecto no cumplido.

El documento se convertirá en una guía procedimental y medio de comunicación, basados en los lineamientos de las normas ISO 27001 que establece los estándares adecuados de seguridad informática y en documento escrito por Salazar[12]

5.5. POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TALENTO HUMANO

Debido a que el mayor riesgo se encuentra en negligencia institucional, iniciamos por las políticas de seguridad informática, para el talento humano, detalladas en el cuadro No. 15, las cuales serán responsabilidad del personal de la Oficina de Planeación y Sistemas, aunque la información interactúe con otras áreas de la compañía que se crean convenientes, los cuales estarán a cargo de difundir el reglamento para el buen uso y mantenimiento, así como también de verificar su cumplimiento.

Debido al carácter confidencial de la información, el personal de la compañía deberá trabajar de acuerdo a los códigos de ética profesional, normas y procedimientos establecidos en los contratos y reglamento de la compañía.

Cuadro No. 15 Políticas de seguridad informática en talento humano.

POLITICA	PORQUE
Todos los trabajadores de la compañía, los usuarios externos y los terceros que desempeñen funciones en los Sistemas de Información, recibirán una adecuada capacitación y actualización periódica en materia de las PSI, normas y procedimientos de los Sistemas de Información	Porque de esta forma se hará conciencia de la importancia de su participación y colaboración en todo el proceso de desarrollo de seguridad de la información
Los usuarios del servicio de correo electrónico deben conocer la importancia del buen uso del mismo y los peligros que la compañía se expone por su mal uso como ataque de virus, intercepción, descargar archivos adjuntos, etc.	Porque esta política ayudara a que los empleados tomen consciencia del buen uso de los recursos y servicios informáticos, también es importante que los empleados sepan los riesgos a los que la compañía está expuesta y como pueden colaborar.
Es necesario que todos los empleados tengan conocimiento de la integridad, disponibilidad, confiabilidad y continuidad de los servicio y bienes más importantes de la compañía como los financieros, comerciales y técnicos que atentan con la continuidad del servicio del negocio.	Porque de esta forma los empleados pueden ayudar a salvaguardar y proteger dichos activos informáticos.

[12]SALAZAR, Trelles, Análisis de riesgos y diseño de políticas de seguridad Capitulo 4. http://dspace.ups.edu.ec/bitstream/123456789/573/6/CAPITULO4.pdf

Cuadro No. 15 (Continuación)

POLITICA	PORQUE
Se debe concientizar a los empleados de la compañía sobre la importancia y las responsabilidades individuales que tiene con la información que manipulan y la compañía le confió.	Porque así cada empleado tendrá los cuidados adecuados de la información que utilizan y manipulan.
Toda persona, empleado fijo u subcontrata (*outsourcing)* que manipule información de la compañía deberá firmar un contrato de confidencialidad amparado por pólizas de contratación y responsabilidad civil.	Porque con esto se pretende proteger la información, de tal forma que esta no sea utilizada en contra de la integridad de la compañía.
Todos los privilegios, claves y permisos otorgados a los empleados subcontrata (*outsourcing*) deben ser bloqueados o eliminados luego de que estos terminen sus actividades de forma definitiva. Además las pólizas de responsabilidad civil deben estar vigentes por un espacio mayor a la terminación del contrato.	Porque en caso de terminar el contrato en malos términos se impedirá que el personal despedido acceda y dañe la información de la compañía o que otras personas accedan a los datos de estos usuarios.
Queda terminantemente prohibido cualquier tipo de actividad o celebración dentro de las áreas en las cuales existen equipos de cómputo, dispositivos o información de la compañía que pudiere afectar la integridad, disponibilidad o confidencialidad de la información.	Porque estos equipos pueden resultar dañados por descuido o derrame de bebidas o alimentos y provocar perdida de información, daño de equipos, suspensión de servicios u ocasionar paro de la producción o actividades.
El documento de las PSI, debe ser difundido a todo el personal involucrado y crear conciencia con capacitación y talleres sin importar el cargo en la compañía en la definición de estas políticas de seguridad informática. Como también al personal nuevo que se contrata temporalmente o reemplazo de vacaciones.	Porque de esta manera se mantendrá informado al personal de la compañía de lo que puede o no puede hacer, lo cual facilitará la implementación del proceso de seguridad informática.

5.6. POLÍTICAS DE SEGURIDAD INFORMÁTICA DE REDES Y TELECOMUNICACIONES

Las políticas de seguridad informática detalladas en el cuadro No 16, serán responsabilidad del personal de la Oficina de Planeación y Sistemas de la compañía, la cual estará a cargo de difundir el reglamento para el uso de la red y de sus componentes, así como también de verificar su cumplimiento.

Cuadro No. 16: Políticas de seguridad informática para Redes y Telecomunicaciones

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
La oficina de Planeación y Sistemas deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, de aplicaciones, del uso de la *Intranet* institucional, así como las especificaciones deben quedar estandarizadas para el acceso a estos sea seguro	Porque de esta forma se administrará de manera correcta todos los servicios que se brindan en la red.

Cuadro No. 16 (Continuación)

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
Se debe evitar todo tipo de publicación de información como: nombre de sucursales, ubicaciones, nombre de dispositivos, marcas y demás, mediante etiquetas o en la configuración de los equipos de red tales como: *routers*, servidores, clientes, etc.	Porque de esta forma se evitará que terceras personas conozcan información sobre la red de la compañía, lo cual dificultará su acceso.
Las contraseñas usadas para la configuración de equipos de redes y telecomunicaciones deberán estar basadas en un estándar que defina aspectos como: estructura, tiempo de validez, reusabilidad, etc.	Porque así daremos mayor seguridad informática a todos los dispositivos informáticos de la compañía, evitando posibles accesos de terceras personas.
Borrar todos los usuarios y contraseñas que vienen por defecto en los equipos informáticos usados en la red como: *Router*, *Switch*, enrutadores, etc, y crear *VLANs* o redes lógicas debidamente estructuradas para mejorar la eficiencia de la red.	Porque de esta forma se dará mayor seguridad informática a la red evitando el fácil acceso de terceros a la red de la compañía, a través de los equipos de red.
Todos los puertos y protocolos de los dispositivos utilizados en la red, que no estén en uso deberán ser bloqueados adecuadamente.	Porque así se le dará mayor protección a la red, evitando ataques ya sean internos o externos, y al mismo tiempo se facilitará la administración de la red
Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red, debidamente codificados e identificados.	Porque de esta forma se facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de red, más aun cuando los responsables de estos equipos no estén.
Al momento de diseñar la red se deberá considerar todas las seguridades y ventajas que los equipos de red estén en capacidad de proveer en lo posible utilizando equipos de alta tecnología.	Porque de esta manera se obtendrá el máximo desempeño de los recursos de red utilizados, mejorando considerablemente la seguridad informática, la administración, y facilidad de mantenimiento.
Todos los dispositivos de red deberán estar correctamente salvaguardados, tomando en cuenta aspectos como ubicación, protección física y suministro eléctrico (de ser necesario).	Porque de esta forma se pretende proteger los dispositivos en lo que a riesgos de tipo físico se refiere, evitando así su deterioro o daños irreparables.
El personal que realiza trabajos de configuración de los dispositivos de red deberá poseer una certificación o título que avale sus capacidades y conocimientos.	Porque de esta forma se garantizará el trabajo realizado, evitando posibles fallas que comprometan a la red de la compañía y la disponibilidad de la información.
Todos los enlaces de red sean estos fijos o redundantes, a través de medios guiados o no, deben ser probados rigurosamente con el fin de garantizar su servicio.	Porque de esta forma se garantiza la conexión entre los dispositivos de red y que la transmisión de datos sea confiable, evitando así la interrupción de servicios
Se debe definir un proceso de reemplazo de equipos, ya sea manteniendo acuerdos con proveedores (precios, tiempo de reposición, disponibilidad) o de ser posible tener unos de respaldo en bodega.	Porque así el tiempo de suspensión de los servicios que el equipo provee será corto y se mantendrá la continuidad del negocio
Se debe implementar enlaces redundantes de las conexiones más importantes para la compañía ya sea para la red interna o para la red externa (*Internet*).	Porque de esta forma se mantendrán disponibles los servicios de la red, evitando la pérdida de datos y demoras en transmisión que puedan afectar la continuidad del negocio.

Cuadro No. 16 (Continuación)

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
El acceso a la *Internet* será restringido, debe ser suministrado solamente para el personal de la compañía que necesite del servicio para realizar labores propias de la compañía.	Porque con esta política se pretende optimizar el uso del servicio de Internet, aprovechando el ancho de banda al máximo, también se evitará que el personal de la compañía realice actividades distintas a las laborales.
El servicio de correo electrónico, tanto interno como externo deberá ser usado única y exclusivamente para intercambio de información de interés empresarial, quedando prohibido la suscripción a cualquier sitio *web* con el *mail* corporativo.	Porque de esta forma se optimizará el uso del correo electrónico y al mismo tiempo se crea una medida de protección contra mail basura y malicioso.
Todos los equipos servidores y equipos de comunicación deberá contar con una instalación auxiliar acondicionada adecuadamente para albergar sus equipos informáticos.	Porque con esta política se pretende darle continuidad al negocio en el caso de que las instalaciones informáticas de la compañía colapsen o no se pueda acceder a las instalaciones
La Oficina de Planeación y Sistema es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso y autenticación a los recursos informáticos disponibles en la compañía.	Porque evitando así el acceso no autorizado a los recursos de la compañía, se previene intuición de acceso no autorizado a la información de la compañía.
Todo *software* que maneje autenticación debe cifrar la información que circule a través de la red.	Porque esto evitara que terceras personas puedan leer fácilmente la información confidencial que circula en la red.

5.7. POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE INFRAESTRUCTURA Y *HARDWARE*

Las PSI detalladas en el cuadro No.17, de este apartado serán responsabilidad del personal de la Oficina de Planeación y Sistemas de la compañía, el cual estará a cargo de difundir el reglamento para el uso de los dispositivos de *hardware*, así como también de verificar su cumplimiento.

Cuadro No. 17. Políticas de seguridad informática para Infraestructura y *Hardware*

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
Cerca de todos los equipos, se deberá ubicar un extintor adecuado para equipos electrónicos, y de no ser posible, al menos cerca de los equipos más importantes.	Porque de esta forma se protegerá la seguridad informática de los equipos en caso de un incendio
Todos los equipos y dispositivos que estén o no en uso tanto de redes y telecomunicaciones, como de *hardware* en general, deberán estar almacenados en un lugar seguro frente a robos, accesos no autorizados y eventualidades que puedan averiarlos.	Porqué de esta manera se pretende proteger físicamente todos los elementos de *hardware* y dispositivos de comunicación de la compañía.

Cuadro No. 17. (Continuación)

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
La Oficina de Planeación y Sistemas le corresponde la realización del mantenimiento periódico preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física en informática, y su acondicionamiento específico. Para lo cual se debería crear un procedimiento formal (fechas, responsables, informe escrito) que especifique la forma en la que se realizará este mantenimiento.	Para que de esta forma se evitara la pérdida de tiempo o complicaciones al momento de dar mantenimiento a los dispositivos, prolongando su vida útil, evitando que personal que no tenga conocimiento técnico manipule los equipos.
Periódicamente deberá actualizarse y llevar un inventario de todos los equipos y dispositivos que formen parte del sistema informático, estén o no en uso, debe incluir parámetros como: fecha de adquisición, proveedor, modelo, manual técnico y de usuario, responsable, garantía, y demás aspectos que la Oficina responsable estime conveniente. Además debe estar acompañado de un documento que describa la configuración y estado actual del equipo, así como de posibles advertencias sobre el buen uso del mismo.	Porque esta forma se podrá administrar con facilidad los activos informáticos de la compañía, conocer su estado actual y disponibilidad en bodega y se pretende lograr la manipulación adecuada de los equipos, y rapidez en su mantenimiento.
Se deberá establecer un control en las áreas principales donde se ubican los dispositivos de gran importancia como: cuartos de servidores o telecomunicaciones, el cual deberá registrar todas las todas las actividades realizadas por el personal que accede a estas áreas.	Porque de esta forma se llevará un control y se conocerá factores como: ¿quién?, ¿para qué? y ¿a qué hora?, ingreso a estas áreas a manipular los dispositivos.
La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos de la Oficina de Planeación y Sistemas, se hará únicamente bajo la autorización de dicha oficina o los responsables designados, se deberá documentar dicho proceso con aspectos como: razones de reubicación, nombre de responsable, equipos reubicados, etc.	Porque de esta forma facilitara la administración del *hardware* y mantendrá actualizado el inventario de activos informáticos.
Todos y cada uno de los equipos serán asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos previa capacitación y puesto en conocimiento	Porque de esta forma se mejorará la administración de los recursos y se facilitará su mantenimiento.
Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no sean propiedad de la compañía	Porque de esta forma la compañía se evitará problemas con los operarios ya que estos únicamente realizarán las labores que les corresponde dentro de la Compañía.

5.8. POLÍTICAS DE SEGURIDAD INFORMATICA PARA EL MANEJO DE *SOFTWARE*

Las PSI detalladas en el cuadro No. 18 de este apartado serán responsabilidad del personal de la Oficina de Planeación y Sistemas y de las subgerencias o áreas responsables de la información de compañía, quienes estarán a cargo de difundir el reglamento para el uso y mantenimiento del *software*, así como también de verificar su cumplimiento.

Cuadro No. 18: Políticas de seguridad informática para el manejo de *software*

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
Todos los computadores utilizados en la Compañía deben tener configurado la opción de cierre de sesión después de un lapso de inactividad (determinado por la oficina de sistemas).	Porque de esta manera se evitará el acceso de usuarios no autorizados a estos computadores, previniendo la pérdida de información
Debe haber una correcta administración de todos los usuarios que tienen acceso a un dispositivo o equipo y los privilegios sobre el sistema operativo y las aplicaciones que opera	Porque así se llevará una correcta administración de los usuarios y de los equipos, previniendo el mal uso de los mismos.
La instalación de *software* básico para cualquier equipo, debe ser instalado por personal de la Oficina de Planeación y Sistemas.	Porque de esta forma se protegerá a todos los dispositivos de la compañía, se evitara que los usuarios instalen *softwar*e malicioso que perjudique a la compañía y se mejorará el control ya que se conocerá que *software* está permitido y cual no.
En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de *software* con licenciamiento apropiado y de acorde a la propiedad intelectual.	Porque así se evitará el uso de aplicaciones o *software* inútil que provoque el mal uso de los recursos o pérdida de información.
Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de *software* de seguridad informática (antivirus, vacunas, privilegios de acceso, y otros que se apliquen), debidamente actualizados	Porque de esta manera se pretende brindar mayor protección a la compañía, evitando la proliferación de virus que puedan suspender los servicios de red u ocasionen pérdida o fugas de información
Todo *software* nuevo antes de ponerlo en uso debe ser probado y evaluado correctamente antes de ponerlo en funcionamiento.	Porque de esta forma se evitará el uso de *software* defectuoso que pueda poner en peligro la integridad o perdida de la información.
Se debe realizar periódicamente revisiones del funcionamiento del *software* e instalación de actualizaciones en caso de que existan	Porque así se pretende aprovechar al máximo el rendimiento de los equipos y prolongar su tiempo de vida útil.
Todo *software* utilizado en la compañía deberá en lo posible tener un manual técnico y de usuario que facilite su uso y mantenimiento. En caso de compra se deberá exigir a sus proveedores, en el caso que esto no sea posible se lo diseñará, y, si el *software* es creado por la compañía los desarrolladores deberán realizar el manual correspondiente.	Porque de esta manera se pretende que el *software* empleado en la compañía sea utilizado correctamente, y que cualquier manteniendo o reparación se lo realice en el menor tiempo posible.
La Oficina de Planeación y Sistemas debe tener un cronograma para realizar revisiones periódicas y asegurar que sólo programación con licencia o programas permitidos estén instalada en los computadores de la compañía	Porque de esta forma se verificara el correcto uso de los computadores y de los recursos informáticos brindados a los usuarios, evitando programas con código malicioso pongan en peligro los servicios de red.
Todos los sistemas programados (programas, bases de datos, sistemas operativos, interfaces) o desarrollados con o a través de los recursos de la compañía y la Oficina de Planeación y Sistemas se mantendrán como propiedad de la compañía.	Para qué de esta manera se evitará que los recursos de la compañía sean mal utilizados.

5.9. POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE DATOS

Las PSI de seguridad informática detalladas en el cuadro No. 19 de este apartado serán responsabilidad del personal de la Oficina de Planeación Sistemas y de las oficinas responsables del manejo de información, las cuales estarán a cargo de promover y difundir el reglamento para el buen uso, respaldo y salvaguarda de los datos digitales o impresos, así como también de verificar su cumplimiento.

Cuadro No. 19: Política de seguridad informática de Datos.

POLÍTICAS DE SEGURIDAD INFORMÁTICA	PORQUE
Todos los datos de gran importancia para la compañía deberán ser respaldados y almacenados en un lugar seguro	Porque de esta forma se protege la información y respaldos en forma física y en caso de desastre se pueda continuar con el negocio.
Se debe incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas.	Porque así se podrá conocer todo lo que pase dentro de la base de datos, y detectar fácilmente posibles agresores.
Todo el personal de la compañía o externo a ella, que manipule información sensible, o respaldos deberá comprometerse a protegerla o firmar un acuerdo de confidencialidad, si es necesario respaldado con una póliza de Responsabilidad	Porque de esta manera se evitará la pérdida, robo, daño y mal uso de la información y también se concientizará al personal de la compañía sobre la importancia del manejo adecuado de esta.
Se debe tener implementado y configurados los computadores con un mecanismo de seguridad informática que controle el acceso del personal de la compañía o terceras personas a datos digitales, impresos, licencias, y demás activos a cargo de la oficina de Planeación y Sistemas.	Porque con esto protegeremos los activos de robos, copias, destrucción y mal uso de los mismos.
Se debe implementar un mecanismo formal que administre y controle la eliminación de información lógica y física	Porque de esta forma evitaremos el mal uso de la información que la compañía descarte.
Toda la información que se maneja dentro del departamento de sistemas deberá estar clasificada según los parámetros que la oficina de Planeación y Sistemas crea conveniente.	Porque de esta manera se facilita su administración y manipulación
Todo el *software* de propiedad de la compañía deberá ser usado exclusivamente para asuntos relacionados con las actividades de la compañía.	Así se evitará que el *software* de la compañía sea mal utilizado.

5.10. POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL SISTEMA ELÉCTRICO

Las PSI detalladas en la cuadro No 20 esta sección serán responsabilidad del personal de la Oficina de Planeación y Sistemas de la compañía, la cual estará a cargo de difundir el reglamento para el buen uso y mantenimiento de los componentes relacionados al sistema eléctrico, así como también de verificar su cumplimiento.

Cuadro No. 20: El sistema eléctrico

POLÍTICAS DE SEGURIDAD INFORMÁTICA	EL PORQUE
El acceso a la fuente eléctrica y corte deberá ser controlado y restringido, solo a personal autorizado, además debe ser revisado periódicamente a igual que cualquier otro equipo *hardware*	Porqué así se garantizará que este dispositivo no sea manipulado o averiado por terceras personas y con el mantenimiento periódico permite garantizar la vida útil o daño fortuito
La instalación eléctrica y el equipamiento auxiliar debe cumplir con norma del Reglamento de Instalaciones Eléctricas (RETIE)	Porque así se evitará que estos causen daño a los usuarios por descuido o intencionalmente, preservando la vida humana y equipos asociados al sistema eléctrico

Cuando las PSI se van a publicar y difundir debe tener en cuenta la construcción de las mismas los siguientes aspectos como: **"Establecer lo que se debe o necesita hacer y porque, pero no él cómo",** ya que el cómo es información confidencial de la compañía. Como filosofía de las políticas de seguridad Informática se tiene que todo lo que no se dice en las PSI está permitido.

6. CONCLUSIONES.

- ✓ El presente proyecto permitió identificar los activos de información agrupados en: activos de información que identifican la información del negocio de la compañía entre otras la más relevantes son: la comercial y financiera. Bases de datos, existentes en 25 servidores entre espejos y redundantes que procesan la información de la compañía para mantener la continuidad del negocio. Software comerciales y desarrollos a la medida que procesan la información y establecen la comunicación del usuario con la base de datos. Servicios que presta, como mantener la información actualizada y en línea para todos los usuarios y clientes de la compañía, verificar: metas, estadísticas de calidad y continuidad del servicio público prestado.
- ✓ Los activos informáticos de la compañía están representados en arquitectura del sistema, configurado como cliente servidor, puntos de conexión como los elementos de comunicación, red, puntos de acceso, puntos de conexión. Equipamientos informáticos (hardware) representado en servidores estaciones de trabajo y equipos portátiles. Se cuenta con servicios subcontratados como el Internet en dos puntos redundantes de la infraestructura de la compañía para garantizar la comunicación. Instalaciones físicas en donde se ubican los equipos informáticos y el activo más importante de cualquier compañía: el personal o talento humano que hace posible la existencia de la compañía.
- ✓ Como resultado del análisis de las encuestas, entrevistas y observación de los activos de información, se encontraron vulnerabilidades muy representativas, entre otras están: el computador en la estación de trabajo es utilizado por más de una persona en un 31.71% de los casos. Falta de capacitación en temas de seguridad informática porque los usuarios afirman conocer los controles de seguridad informática en un 53.66%, lo que indica que el 46,44% restante los desconocen, esto significa que en general el conocimiento y aplicabilidad son deficiente. En cuanto a la combinación de caracteres utilizados en las contraseñas para el acceso a los sistemas informáticos, existe una deficiencia del 7,32% que utilizan nombre y fechas conocidas, lo que permite mediante ingeniería social descubrir la clave de acceso de estos usuarios. Además, el 9.72%. de

los usuarios utilizan una cantidad de caracteres menores a seis. Si bien es cierto, los porcentajes son bajos, considerando que se trata de seguridad informática, cada caso cuenta.

- ✓ Otras de las vulnerabilidades más representativa es el manejo de la información por fuera de la compañía en un 51.22%, lo que coloca en peligro la integridad y confidencialidad de la información. En las aplicaciones que manejan los usuarios el 31.71% tiene privilegios de borrado, actualización y creación de nuevos registros. La vulnerabilidad más representativa, según las entrevistas a los administradores, es que ninguno realiza monitoreo a los logs de actividades de los clientes. Además, estos servidores son configurados por terceras personas, lo cuales tiene una vinculación de suministro con la compañía, lo que implica poca responsabilidad.
- ✓ También se pudo identificar las amenazas más representativas que pueden afectar los activos informáticos, ente ellos están: sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales, originadas por muchos factores como falta de capacitación en seguridad informática y responsabilidad informática, falta de definición de privilegios y restricciones del perfil del personal. Amenazas de origen físico como inundaciones, sobrecargas eléctricas, falta de ventilación. Otro grupo de amenazas como criminalidad común y motivación política, producida por los factores como extorción, estafa, vandalismo, robo electrónico y virus.
- ✓ Como consecuencia de la existencia de vulnerabilidades en los activos de información y la probabilidad de ocurrencia de una amenaza, el riesgo se vuelve eminente dañando los activos y causando pérdidas en los activos de información por incidentes ocurridos en la compañía como: la lentitud en los procesos y aplicaciones evidenciada 58.54% de los equipos, pérdida en la conexión 51.22%, ataques de virus informáticos con una ocurrencia de 43.90%, Pérdida de información el 17.07% , discontinuidad en algunos de los servicios corporativos con el 58.54%, etc. Estos incidentes dañan la imagen y la economía de la compañía por afectar uno de los pilares de la seguridad informática.
- ✓ La compañía tiene un sistema de seguridad informática que contempla algunos apartes de la norma estándar ISO NTC 27001, implementada como controles de seguridad de

la información en los procesos de calidad de la ISO NTC 9001, con unas políticas de seguridad informática llamados controles que fueron analizadas en el resultado de la encuesta, dando respuesta a una de las sub preguntas de aplicabilidad de PSI implementadas, encontrándose debilidades en cuando a la poca difusión y capacitación en la implementación del sistema de seguridad informática.

- ✓ Ante la debilidad anterior, se elabora un plan de capacitación y difusión de las políticas de seguridad informática que tiene como finalidad sensibilizar, concientizar a los usuarios\(as) de la importancia y apropiación de las PSI, para bridar seguridad a los activos de información, por lo cual debe ser un compromiso de todos los usuarios de la compañía de PROPOLSINECOR.
- ✓ Como resultado del estudio y análisis de la información obtenida en las encuestas entrevistas y análisis documental, se ha diseñado políticas de seguridad informática normativas y procedimientos de buenas prácticas, para proteger y salvaguardar la información y los sistemas informáticos de la compañía, explicando el porqué de esta PSI, con el único fin de concientizar y sensibilizar a los usuarios (as), la importancia de, la aplicabilidad de las políticas de seguridad informática en la compañía de PROPOLSINECOR.
- ✓ Los beneficios obtenidos con la elaboración del presente trabajos fueron: identificar los principios de seguridad, objetivos, obligaciones en función de la legislación aplicable y protección del patrimonio; continuidad y coherencia de las acciones de seguridad informática en cada una de las actividades, especialmente para toda elección técnica en la adquisición de equipos, pero también organizacional o contractual, aplicación de principios y normas de seguridad que deben tenerse en cuenta para el normal desarrollo de las actividades, creación de conciencia sobre el riesgo que amenazan a los sistemas de información y sobre los medios disponibles para protegerse de los posibles ataques y las responsabilidad que implica el incumplimiento de las políticas de seguridad informática.

7. RECOMENDACIONES.

Con base en los resultados de la presente investigación se puede realizar las siguientes recomendaciones, destacando los aspectos más notables o relevantes de lo definido en apartes del documento:

Segmentación de red.

La compañía ha segmentado la red de algunas áreas, debido a la importancia que la totalidad de la red corporativa quede segmentada con la creación de *VLANs* ya que se la puede realizar sobre los dispositivos que la compañía posee, siendo una alternativa económica crear subredes por áreas facilitando la administración y el rendimiento de la red, de esta forma la seguridad informática de la red incrementará considerablemente.

Cierre de sesión.

Conociendo que el 39% de los usuarios no tiene la precaución de cerrar la sesión ante ausencia temporal, se creó la política **"Todos los computadores utilizados en la Compañía deben tener configurado la opción de cierre de sesión después de un lapso (determinado por la oficina de Planeación y Sistemas) de inactividad"** es muy importante que después de un tiempo máximo de inactividad (de 3 a 5 minutos), el computador cierre sesión, lo cual impedirá que terceros accedan a información o aplicaciones que no les pertenece incrementando la seguridad informática.

Capacitación. Como una de las debilidades más notorias en el análisis de riesgos es la impericia y negligencia de los usuarios en el manejo de datos e información, ante esto es muy importante la implementación del plan de sensibilización y concientización de las PSI y tener en cuenta las PSI creadas en talento humano, datos e información principalmente la que dice: **"Todos los trabajadores de la compañía, los usuarios externos y los terceros que desempeñen funciones en los Sistemas de Información, recibirán una adecuada**

capacitación y actualización periódica en materia de las PSI, normas y procedimientos de los Sistemas de Información".

Administración. La administración de base de datos y aplicativos no se encuentra estandarizada y cada uno administra a su manera y de acuerdo a sus conocimientos, sin seguir un proceso, esto hace débil la administración, principalmente en el control de acceso y el monitoreo de base de datos de información sensible, además la administración se encuentra en manos de terceros, esto hace más vulnerable la información, por eso se plantea la siguiente política para tenerla en cuenta **"Todo el personal de la compañía o externo a ella, que manipule información sensible, o respaldos deberá comprometerse a protegerla o firmar un acuerdo de confidencialidad, si es necesario respaldado con una póliza de Responsabilidad".**

En el proceso de investigación se pudo establecer que hace falta una estructura jerárquica dedicada exclusivamente al manejo de la seguridad de la información, como también herramientas que permitan monitorear la red y probar la vulnerabilidad de los aplicativos.

REFERENCIAS BIBLIOGRAFICAS.

- ÁLVAREZ MARAÑÓN. Gonzalo (2009), Como protegernos de los peligros de internet. CSIC.
- AMAYA TARAZONA. Carlos Alberto. 2013. Seguridad en aplicaciones Web. Universidad Nacional Abierta y a Distancia. Duitama.
- CAN/CSA-ISO/IEC TR 13335-1-01 Information Technology - Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security (Adopted ISO/IEC TR 13335-1:1996, first edition, 1996-12-15) STANDARD published 03/26/2001 by Canada National Standard/Canadian Standards - ISO/IEC
- CANO, Jeimy J. (2004) Auditoria de Seguridad, Evaluación de Seguridad y Pruebas de Penetración: Tres Paradigmas en la Seguridad Informática
- CAVIEDES SANABRIA, Fernando. PRADO URREGO, Bertulfo, (2012). Modelo Unificados para identificación y valoración de los riesgos de los activos de información en una organización, Universidad ICESI Santiago de Cali,
- CERTICAMARA. ABC para proteger los datos personales Ley 1581-2012 decreto 1377 de 2013. https://www.certicamara.com
- CRUZ MENDOZA, Erik Ivan. RODRIGUEZ DUQUE, Diana Vanessa. (2010). Modelo de Seguridad para la Medición de Vulnerabilidades y reducción de Riesgos en Redes de Datos. Intitulo Politécnico Nacional UNIICSA. México
- DE FRAITAS. Vidalina. 2009. Análisis y evaluación del riesgo de la información: caso de estudio Universidad simón Bolívar
- Erik Ivan CRUZ y Diana Vanessa RODRÍGUEZ del Instituto Politécnico en la ciudad de México, en noviembre de 2010 realizan la tesis de grado titulada
- GOMEZ GALLO (2005), Luis Humberto Presidente del senado. (2005) Ley 962 de 2005. Diario oficial 45.963. http://www.ani.gov.co/sites /default/files/ley_0962_de_2005_ racionalización _de_tramites_y_procedimeitnos_administrativos.pdf.

- GUERRA DE LA ESPRIELLA, María del Rosario. (2009). De las telecomunicaciones a las TIC Ley de TIC de Colombia LEY 1341/09 Bogotá Colombia
- GUERRA DE LA ESPRIELLA, María del Rosario. Resolución No. 2258 de 2009. La Comisión de Regulación de Comunicaciones (CRC) Republica de Colombia.
- HERNÁNDEZ PINTO. María Gabriela. (2006). El proyecto tesis. Diseño de un Plan Estratégico de Seguridad de Información en una Empresa del Sector Comercial.
- INCONTEC. (2006) Norma Técnica Colombiana. NTC-ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI) requisitos
- COLINAS RAMÍREZ, Jorge (2008). Plan de seguridad, para una pequeña. Universidad Pontificia Comillas, Madrid España, en septiembre del 2008.
- JUAN CARLOS I REY ESPAÑA. (2007) Ministerio De La Presidencia: María Teresa Fernández de la Vega Sanz. Ley 11 de 2007 de 4 junio. de acceso electrónico de los ciudadanos a los Servicios Públicos. http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html#i
- LA BACA CASTRO, Raphael. El Universal. Las Tendencias en Seguridad Informática para el 2014. Encontrado en: http://www.eluniversal.com.co/tecnologia/las-tendencias-en-seguridad-informatica-para-el-2014-143079
- La Superintendencia Financiera de Colombia. (2007). CIRCULAR EXTERNA 052 DE 2007. Capitulo Décimo Segundo: Requerimientos Mínimos De Seguridad y Calidad en el Manejo de Información a Través de Medios y Canales de Distribución de Productos y Servicios. Entra en vigencia mediante tres etapas: la primera inicia el 1º de julio de 2008, la segunda el 1º de enero de 2009 y la ultima el 1º de enero de 2010.
- LLABRES. Francisco.(1998) ISASA-Cobit Gobierno de las TIC, Auditoría y control
- HERNÁNDEZ PINTO, María Gabriela (2006). Tesis Diseño de un Plan Estratégico de Seguridad de Información en una Empresa del Sector Comercial. Escuela Superior Politécnica Del Litoral, en Guayaquil Ecuador
- MEGIAS TEROL, Javier (2008). Gestión Estratégica de seguridad en una empresa. Editorial Etecom.

- NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de la Gestión de la Seguridad de la Información (SGSI) Requisitos. Norma Técnica Colombina. Incontec Internacional.
- NTC-ISO/IEC 27002 Tecnología de la Información. Técnicas de Seguridad. Código de Practica para la Gestión de la Seguridad de la Información. Norma Técnica Colombina. Incontec Internacional.
- PALTA VELASCO. Eleonora Mag. Febrero 2012. Introducción a la Seguridad en Redes. Universidad Nacional Abierta y a Distancia
- ROMERO, Luis Alonso. (2003) Catedrático de Ciencia de la Computación e Inteligencia Artificial de la Universidad de Salamanca. Seguridad Informática Conceptos Generales
- SALAZAR, Trelles, Análisis de riesgos y diseño de políticas de seguridad Capitulo 4. http://dspace.ups.edu.ec/bitstream/ 123456789/573/6/CAPITULO4.pdf
- SANDRA DE SERRANO, Hernán, Presidente del senado. (2007). Ley 1150 de 2007 Diario Oficial. http://acueductopopayan.com.co/ wp-content/uploads/2012/08/ley-1273-2009.pdf
- VEGA. Jesús Emiro. (2012). Módulo de Seguridad en Bases de Datos. Universidad Nacional Abierta y a Distancia
- WILLIAMS, Jeff y WICHERS, Dave. OWASP The Open Web Application Segurity Proyect. OWASP Top 10-2013. Los diez riesgos más críticos en Aplicaciones Web. Aspect Security https://www.owasp.org/ index.php/ Top_10_2013-Top_10.

ANEXOS

ANEXO No. 1: INVENTARIO DE DOCUMENTOS QUE SOPORTAN LA SEGURIDAD INFORMÁTICA DE LA COMPAÑÍA.

A continuación se detallan cada uno de los documentos que soportan el sistema de Gestión de la seguridad informática, dando una breve descripción del documento referenciado.

- **CARACTERIZACIÓN PROCESO DE GESTIÓN SOFTWARE, HARDWARE Y COMUNICACIONES**

El documento establece el proceso, alcance, objetivo, responsable equipo de trabajo, recursos disponibles, proveedores, entradas, actividades, salidas y clientes, como se precisa en el siguiente cuadro:

Cuadro No. 1: Caracterización proceso gestión software, hardware y comunicaciones.

CARACTERIZACION PROCESO GESTION SOFWARE, HARWARE Y COMUNICACIONES		
PROCESO	ALCANCE	RESPONSABLE DEL PROYECTO
GESTION SOFTWARE, HARDWARE Y COMUNICACIONES	DEPARTAMENTO DE NARIÑO	JEFE OFICINA
OBJETIVO	ASEGURAR LA CONTINUIDAD Y CONFIABILIDAD DE LO SOFTWARES, EQUIPOS DE CÓMPUTO Y COMUNICACIONES MEDIANTE LA PLANIFICACIÓN, EJECUCIÓN, CONTROL Y MEJORA DEL PROCESO	
EQUIPO DE TRABAJO		RECURSOS
JEFE OFICINA PLANEACION Y SISTEMAS, PROFESIONAL ESPECIALIZADO SIIF, PROFESIONAL I SISTEMAS, PROFESIONAL DE APOYO SISTEMAS, TECNICO AUXILIAR, COMITÉ DE SISTEMAS, PROFESIONAL I SISTEMAS		SOFTWARE, HARDWARE, EQUIPO DE COMUNICACIÓN, FIBRA OPTICA, PROVEEDORES
RQUISITOS		
LEGALES	NORMATIVOS	CONTRACTUALES
CONSTITUCION POLITICA, LEY 142 Y 143 DE 1994	ACTOS ADMINISTRATIVOS DEL MINISTERIO DE LAS TIC.	ESTATUTOS DE CONTRATACION

- **INSTRUCTIVOS**

  - El instructivo No 1, llamado: administración de usuarios que manejan portales bancarios, cuyo objetivo es atender y dar soporte a los diferentes usuarios que manejan los portales bancarios, con el fin de asegurar el normal desarrollo de sus actividades. El alcance aplica a los trabajadores de la Subgerencia Administrativa y Financiera, Oficina de Tesorería y Oficina de Recaudos especificando las actividades del administrador frente a los usuarios de los portales bancarios.
  - **El instructivo No. 2**, llamado Atención y Soporte a los Computadores que Manejan Portales Bancarios, este instructivo como su título lo dice, brinda atención y soporte para realizan operaciones electrónicas en los portales bancarios de la oficinas de la tesorería de la compañía.

- **FORMATOS:**
  - **Formatos cronograma de mantenimiento,** el formato incluye una programación que se realiza para el mantenimiento anual por sedes y seccionales a los equipos existentes en cada área, donde se especifica el equipo fecha inicial, fecha final y el responsable del mantenimiento.
  - **Formato único de mantenimiento equipos de cómputo,** en este formato se especifica fecha datos usuario, datos equipo, diagnóstico, evaluación, tipo de servicio, servicio realizado y firmas de los participantes.
  - **Formato de control y custodia de copias de seguridad del sistema financiero**. En este formato se registra las entregas diarias de copias de seguridad del sistema financiero, en donde se especifica:

Cuadro No. 2: Copias de seguridad informática

No.	Mes	Nombre Archivo	Fecha de Entrega	Fecha Reintegro	Responsable Entrega	Responsable Recepción
1						

  - **Formato de autorización de acceso al sistema financiero** especificando el tipo el contrato fecha y el tipo de proceso de asignación en la que se especifica sobre cuál de los tres roles de debe autorizar el acceso Menú, Oracle y SQL y al final las firmas de quien solicita y autoriza.
  - **Formato de mejoras a la aplicación del sistema financiero** en donde se especifica la dependencia el cargo el diagnostico la solución o mejora al aplicativo firmada por el solicitante y él que autoriza la mejora.
  - **Formato de reporte de fallas de comunicación**, donde se especifica el nombre de la persona que reporta la falla, lugar fecha y hora de inicio de falla y la fecha y hora de solución, la compañía responsable de la falla, causa y comentarios. Formato de seguimiento soporte técnico, especificando el solicitante la causa y el responsable del soporte técnico, teniendo en cuenta los tiempos de un proceso a otro hasta finalizar.

- **DOCUMENTOS INTERNOS**.
  - **Plan de contingencia al área financiera**, busca reaccionar eficazmente ante cualquier interrupción de uno de los procesos financieros, con el fin minimizar desastres y mitigar los riesgos, para lo cual se nombran responsables y los posibles daños causados especificando el proceso para restablecer el servicio afectado al Sistema de Gestión de la Seguridad de la Información.

- **PROCEDIMIENTOS ESTABLECIDOS**
  - **Copias de seguridad informática**, asignan responsable, periodicidad y lugar donde se custodia la información.

- **Expedición de paz y salvo a empleados** que han tenido acceso al sistema de información.
- **Mantenimiento preventivo** a los equipos de cómputo asignando responsables y cuyo objetivo prevenir posible ocurrencias de daños.
- **Asignación de usuarios al sistema de información comercial**, para lo cual se ilustra el procedimiento de solicitud y asignación de privilegios y el responsable de la asignación
- **Procedimiento de asignación de módulos a usuarios del sistema comercial.** Ilustra de manera didáctica la asignación de usuarios que harían uso del aplicativo de información comercial a través de los diferentes módulos que se hayan autorizado previamente.
- **Procedimientos para la custodia de libros principales *bakup*** y protección de información base de datos del sistema financiero.
- **Procedimiento de exportación de información del sistema comercial a las tablas**, auditoria campos, auditoria tablas, copias de seguridad informática, para realizar estudios, investigaciones análisis etc.
- **Procedimiento de actualización de versiones de programas fuentes del sistema financiero** se mantenga respaldos y estos se puedan modificar o actualizar fácilmente en el momento que los necesite.
- **Procedimiento para la preparación de servidor de contingencia del sistema financiero** los cuales tiene los respaldos y que serán fácilmente recuperables en el momento que se necesite activar el plan de emergencia.
- **Procedimiento para generar copias de seguridad informática de usuarios finales** y hasta el almacenamiento.
- **Seguridad física y acceso a los servidores** la cual define las actividades necesarias para realizar de manera segura y controlada el acceso a los servidores.

❖ **EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI**.

El documento tiene un alcance que se enmarca en el cumplimiento general de las disposiciones legales vigentes, con el objeto de garantizar adecuadamente la seguridad de la información, los sistemas de información, dominios, procesos y el ambiente tecnológico de la compañía, como parte de la cultura Empresarial en pro del principio de Política de Seguridad informática con el compromiso de las autoridades máximas de la compañía. En la cual forman el comité de sistemas e identifican los activos sensibles de la compañía y toman unos partes de la norma ISO 27001 para armar las políticas se seguridad que no se difundieron adecuadamente a los usuarios internos y externos de la compañía.

ANEXO 2 RESULTADO ENCUESTA

PREGUNTA	RESPUESTAS	CANTIDAD	VALOR %
computador?	e) No lo apaga ni lo bloquea	1	2.44%
	f) Solo se apaga cuando termina la jornada	6	14.63%
9) ¿Por labores propias de su desempeño en el trabajo de la organización?	a) Procesa información fuera de la empresa,	10	24.39%
	b) Se conecta a través de escritorio remoto al computador de la compañía,	6	14.63%
	c) Recibe asesoría a través de escritorio remoto	5	12.20%
	d) No requiere conectarse remotamente	16	39.02%
	e) No requiere llevar información a su casa	9	21.95%
	f) Lo trabaja en horario extendido en la empresa	23	56.10%
	no sabe no responde	1	2.44%
10) En su computador de trabajo, ha sufrido incidentes como:	a) Ataque de virus informáticos	18	43.90%
	b) Perdida de información	7	17.07%
	c) Lentitud en los procesos o aplicaciones	24	58.54%
	d) Perdida de conexión con algún aplicativo	21	51.22%
	e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, etc.	24	58.54%
	f) Daño en su equipo de trabajo	3	7.32%
	g) Ninguno de los anteriores	6	14.63%
11) La frecuencia con que ha sucedido los incidentes en su equipo de trabajo es:	a) A diario	1	2.44%
	c) Cada mes	12	29.27%
	d) Cada tres meses	6	14.63%
	e) Cada seis meses	3	7.32%
	f) Cada año	6	14.63%
	g) Más de un año	9	21.95%
	No sabe no responde	4	9.76%
12) ¿Qué tipo de aplicaciones corporativas o servicios maneja desde su computador ?	a) Aplicación del área financiera	10	24.39%
	b) Aplicación del área comercial (facturación)	19	46.34%
	c) Aplicaciones de control de elementos específicos y técnicos de la organización	6	14.63%
	d) Aplicación de indicadores o cuadros de mando	16	39.02%
	e) Aplicación de control documental	25	60.98%
	f) Aplicaciones de comunicación	9	21.95%
	g) Aplicación de control de atencion al cliente	6	14.63%
	h) Aplicación de nomina	2	4.88%
	i) Aplicaciones de navegación en internet	26	63.41%
	j) Herramienta de desarrollo	3	7.32%
	k) Consulta directa a la base de datos mediante SQL server	12	29.27%
	l) Aplicaciones para el control de proyectos y seguimiento de metas	5	12.20%
	n) Aplicaciones de acceso a escritorio remoto	25	60.98%
13) En el aplicativo que maneja tiene derecho a:	a) Adicionar nuevos registros, b) Actualizar registros, c) Borrar registros, e) Consultar registros	13	31.71%
	a) Adicionar nuevos registros, b) Actualizar registros, e) Consultar registros	6	14.63%
	a) Adicionar nuevos registros, e) Consultar registros	3	7.32%
	b) Actualizar registros	2	4.88%
	b) Actualizar registros, e) Consultar registros	1	2.44%
	d) Consultar registros	14	34.15%
	no sabe no contesta	2	4.88%

ANEXO 2 RESULTADO ENCUESTA

PREGUNTA	RESPUESTAS	CANTIDAD	VALOR %
14) ¿De que programas / archivos hace copia de seguridad?	Archivos varios	8	19.51%
	BBDD	3	7.32%
	Datos empresariales	11	26.83%
	Documentos	3	7.32%
	Documentos excel	4	9.76%
	Excel	3	7.32%
	Informes	2	4.88%
	No sabe no responde	7	17.07%
15) ¿Con que frecuencia se saca copia?	a) A diario	4	9.76%
	b) Cada semana	5	12.20%
	c) Cada mes	8	19.51%
	d) Cada trimestre	11	26.83%
	e) Cada semestre	7	17.07%
	f) Cada año	2	4.88%
	No sabe no responde	4	9.76%
16) ¿Sobre qué programas /aplicaciones ha recibido capacitación?	Administracion de Sistemas Tecnicos	7	17.07%
	Administracion Documental	16	39.02%
	Gestion de Calidad	6	14.63%
	Manejo de equipo tecnico via remota	2	4.88%
	Ninguno	5	12.20%
	Office	2	4.88%
	Sistema de Informacion Comercial	15	36.59%
	Sistema fianciero	6	14.63%
	Sofware calulador de tarifas	1	2.44%
	Todas las anteriores	1	2.44%

ANEXO No. 3. ANÁLISIS DE LA ENCUESTA

La experiencia se llevó a cabo con un grupo de usuarios de la compañía de PROPOLSINECOR conformado por 90 usuarios de los cuales 41 usuarios voluntariamente llenaron la encuesta. Explorando los perfiles de los usuarios encuestados del sistema informático se estima una población heterogénea como:

a) Administrador	8
b) Directivo	3
d) Usuario Final Interno	28
f) Programador /desarrollador	2

Localización en la ciudad de San Juana de Pasto en la compañía PROPOLSINECOR, a la encuesta fue desarrollada a través del correo corporativo, utilizando google drive, la cual se mantuvo al aire por espacio de 9 días calendario entre el 1 y 9 de julio de 2014.

La encuesta de carácter analítico se utilizó para establecer un estudio de tipo cuantitativo, permitiendo conocer la cantidad de usuarios que hacen uso de las políticas se seguridad informática, establecer conductas, vulnerabilidades y amenazas informáticas que se pueden presentar por negligencia de los usuarios del sistema informático.

.

La encuesta no estadística (censo) fue difundida a los 90 usuarios que poseen correo corporativo (total de la población) y respondieron voluntariamente 41 usuarios, a partir de este número se inicia el análisis.

Analizando el resultado de la encuesta se identifica diferentes variables como: la información que se maneja, hábitos de los usuarios, seguridad informática de acceso, vulnerabilidades, políticas de seguridad informática, etc. respuestas a la encuesta y se obtiene los siguientes resultados:

Pregunta ***1) ¿Qué relación laboral tiene con la compañía? Vs 2) ¿Qué perfil tiene en los sistemas de informáticos?*** Se puede concluir que a la encuesta dieron respuesta usuarios heterogéneos dando cubrimiento a todos los perfiles existentes en la compañía, lo más destacado es la vinculación de administradores en los sistemas de contratación laboral, como se puede apreciar en el siguiente cuadro:

Cuadro No. 1: Perfil de los entrevistados

1) ¿Qué relación laboral tiene con la compañía?	2) ¿Qué perfil tiene en los sistemas de información?	cantidad	valor porcentual
a) Contrato a término indefinido	a) Administrador	5	12,20%
	b) Directivo	3	7,32%
	d) Usuario Final Interno	17	41,46%
	f) Programador /desarrollador	1	2,44%
Subtotal		26	63,41%
b) Contrato a término fijo	a) Administrador	2	4,88%
	d) Usuario Final Interno	8	19,51%
	f) Programador /desarrollador	1	2,44%
Subtotal		11	26,83%
c) Contrato de prestación de servicios	a) Administrador	1	2,44%
	d) Usuario Final Interno	3	7,32%
Subtotal		4	9,76%
Total general		41	100,00%

En resumen se identifican los siguientes perfiles que se indican en el siguiente cuadro No 2:

Cuadro No. 2: Resumen perfil encuestados

¿Qué perfil tiene en los sistemas de informáticos?	Cantidad	%
a) Administrador	8	**19,51%**
b) Directivo	3	**7,32%**
d) Usuario Final Interno	28	**68,29%**
f) Programador /desarrollador	2	**4,88%**
Total general	**41**	**100,00%**

Pregunta: ***3) ¿Su computador en el trabajo es utilizado por?*** En las respuestas se puede observar que el 31.71% es compartido con otras personas evidenciándose una vulnerabilidad con la información contenida en el la estación de trabajo, los resultados de la pregunta se indican en el siguiente cuadro No. 3:

Cuadro No. 3: Vulnerabilidad de la impericia del usuario

3) ¿Su computador en el trabajo es utilizado por?	**Cantidad**	**Valor %**
a) Solo por usted	28	68,29%
b) Usted y su compañero de confianza	6	14,63%
c) Tres o más personas	3	7,32%
d) Con usuarios invitados o anónimos de vez en cuando.	4	9,76%
Total general	**41**	**100,00%**

Una de las preguntas que nos brida luces sobre el conocimiento de políticas de seguridad Informática es la pregunta: ***4) ¿De los siguientes controles de seguridad informática, cuales aplican en su trabajo?*** A la cual responden 39 encuestados que conocen alguna de las PSI llamados controles por la compañía y 2 encuestados no responden, ante esto se observa que ninguna de las PSI es aplicada en su trabajado al 100% , la máxima llega al 80.49% y en promedio los controles son conocidos solo en un 53.66% del total de las PSI, el valor porcentual se obtiene en base al número de encuestados 41 usuarios, el resultado de cada una de las PSI se observa en el siguiente cuadro No. 4.

Cuadro No. 4: Controles en la compañía.

4) ¿De los siguientes controles de seguridad informática, cuales aplican en su trabajo?	Cantidad	Valor %
a) Control sobre el uso general del computador en el trabajo,	31	75,61%
b) Control para el uso de dispositivos de almacenamiento externo (memorias USB)	33	80,49%
c) Control para el manejo de claves de usuario	33	80,49%
d) Control para el uso de enlaces Inalámbricos	9	21,95%
e) Control para el uso del internet www	33	80,49%
f) Control para realizar copias de seguridad de la información	26	63,41%
g) Control en el uso del correo electrónico.	26	63,41%
h) Control para el cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales	26	63,41%
i) Control sobre el resguardo y protección de la información	23	56,10%
j) Control para el mantenimiento del computador	18	43,90%
k) Control para dar de baja un equipo de cómputo o periférico	28	68,29%
l) Control para modificar o cambiar configuraciones en el computador	10	24,39%
m) Medidas disciplinarias por incumplimiento de controles informáticos.	23	56,10%
n) Medidas disciplinarias por incumplimiento de PSI.	9	21,95%
no sabe no responde	2	4,88%
Promedio		53,66%

Teniendo en cuenta el número de respuestas afirmativas sobre la aplicación de políticas de seguridad informática en la compañía se obtiene la siguiente gráfica No. 1.

Pregunta: ***5) ¿En cuanto a la instalación de programas o aplicaciones?,*** la respuesta que más llama la atención es la del literal a) con un 12.20% como se indica en el cuadro No 5, lo cual crea vulnerabilidades por instalar programas no autorizados en el computador, que pueden causar o generar daños a la información de la compañía, ya que pueden ser programas piratas o traer anexo virus ,troyanos o programas espías, como se indica en la

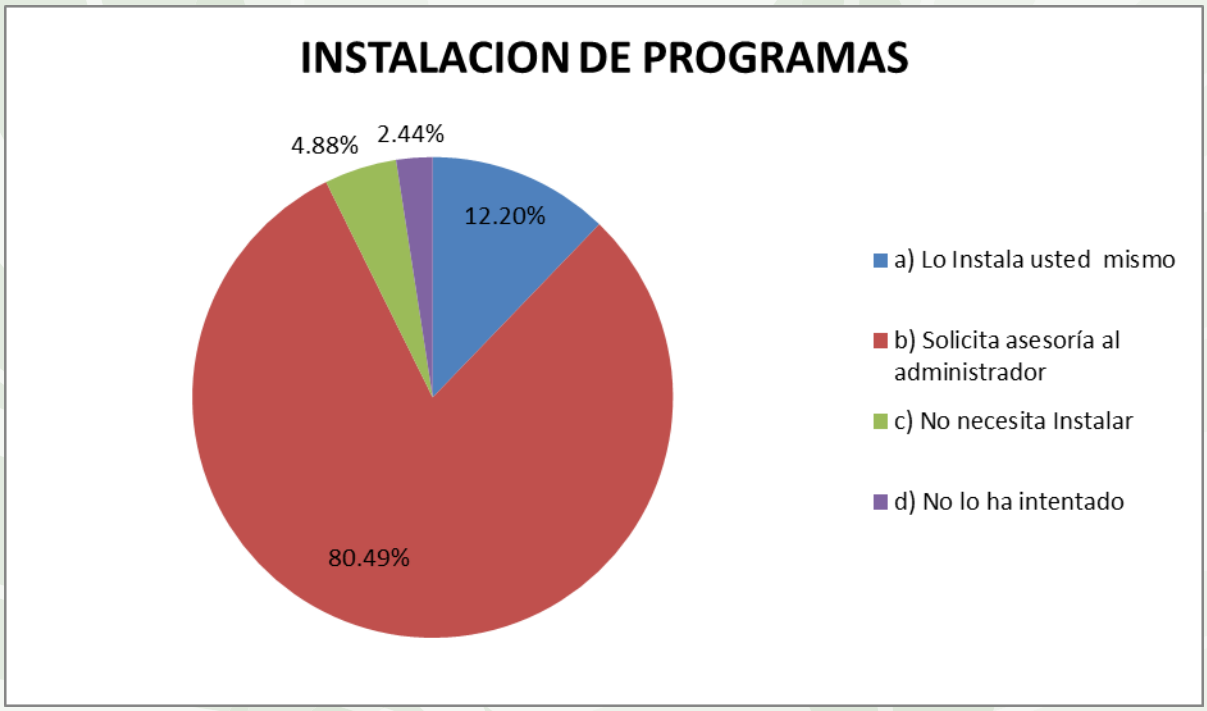
siguiente grafica de color azul, este valor debe minimizarse realizando auditorias y verificando el licenciamiento de los programas.

Grafica No 1 Políticas de seguridad informática

Cuadro No. 5: Instalación de programas

5) ¿En cuanto a la instalación de programas o aplicaciones?	Cantidad	Valor %
a) Lo Instala usted mismo	5	**12,20%**
b) Solicita asesoría al administrador	33	**80,49%**
c) No necesita Instalar	2	**4,88%**
d) No lo ha intentado	1	**2,44%**
Total general	**41**	**100,00%**

También se puede apreciar el resultado en la gráfica No. 2.



Grafica No. 2. Instalación de programas

Pregunta***: 6) ¿Para el manejo de contraseñas de su equipo y/o programas, que tipo de combinación de caracteres utilizas?***, como política de acceso al sistema de información se obtiene un 92.69% de seguridad informática en cuanto a la combinación de caracteres en las contraseñas, pero siempre existe el usuario descuidado que está representado en el 7,31% de los encuestado, que no utiliza la combinación correcta para evitar acceso no autorizados por terceras personas, utilizando el nombre y contraseña del usuario autorizado ante el sistema de información, como se indica en el cuadro No.6.

Cuadro No. 6: Control de acceso.

6) ¿Para el manejo de contraseñas de su equipo y/o programas, que tipo de combinación de caracteres utilizas?	**Cantidad**	**Valor %**
a) Solo nombres conocidos	2	**4,88%**
b) Fechas conocidas	1	**2,44%**
f) Combinación de letras y números	33	**80,49%**
g) Combinación de todo tipo de caracteres	5	**12,20%**
Total general	**41**	**100,00%**

Pregunta ***7) ¿Cuantos caracteres o letras utiliza para sus contraseñas?,*** este factor importante en la utilización de contraseñas, como respuesta se observar el 90, 24 % de las personas encuestadas maneja una seguridad informática de norma, que son más de seis caracteres y el 9, 76% menos de seis caracteres, esto podría representar una debilidad cuando algún extraño trata de averiguar el nombre de la contraseña que por diccionario o fuerza bruta tarda menos tiempo en conseguirlo, el resumen de la encuesta se parecía en cuadro No 7.

Cuadro No. 7: Fortaleza en el control de acceso.

7) ¿Cuantos caracteres o letras utiliza para sus contraseñas?	**Cantidad**	**Valor %**
b) Entre cuatro y seis	4	9,76%
c) Entre siete y nueve	30	73,17%
d) Entre diez y doce	4	9,76%
e) Más de doce caracteres	3	7,32%
Total general	41	100,00%

Tenido en cuenta que la ingeniería social aprovecha descuidos de los usuarios se plantea la siguiente pregunta: ***8) ¿Cuándo se ausenta temporalmente de su estación de trabajo, el computador?*** Los resultados se indican en el cuadro No. 8.

Cuadro No. 8: Descuidos de los usuarios.

8) ¿Cuándo se ausenta temporalmente de su estación de trabajo, el computador?	**Cantidad**	**Valor %**
a) Lo deja apagando	10	**24,39%**
b) No lo apaga y se bloquea automáticamente	15	**36,59%**
c) No lo apaga y lo deja bloqueando manualmente	9	**21,95%**
e) No lo apaga ni lo bloquea	1	**2,44%**
f) Solo se apaga cuando termina la jornada	6	**14,63%**
Total general	**41**	**100,00%**

Teniendo en cuenta las respuestas de los encuestados, el personal tiene un alto grado de cuidado en proteger su computador en caso de ausencia y solo el 2.44 % no lo apaga ni lo bloquea y el 14,63% solo lo apaga cuando termina la jornada, ante esto se debe corregirse y configurar los equipos, que al detectar inactividad sean bloqueados automáticamente, puede representar vulnerabilidad, que puede ser aprovechada por personas inescrupulosas.

El activo más importante en una compañía es la información, tenido en cuenta esto se realizó la siguiente pregunta ***9) ¿Por labores propias de su desempeño en el trabajo de la***

compañía? Analizando las respuestas en cuadro No. 9, se puede concluir que existe vulnerabilidades en el proceso, ya que el 24.39% de la información es procesada fuera de la compañía, el 14.63% se conecta a través de escritorio remoto con aplicaciones gratuitas y no controladas por el administrador, con el fin de ingresar a las aplicaciones propias de la compañía y el 12.20% recibe asesoría externa a través de escritorio remoto, en conclusión existe vulnerabilidades para procesar la información fuera de la compañía, generando una amenaza que atenta contra la confidencialidad e integridad de la información.

Cuadro No. 9: Vulnerabilidades en la información

9) ¿Por labores propias de su desempeño en el trabajo de la compañía?	**Cantidad**	**Valor %**
a) Procesa información fuera de la compañía,	10	24,39%
b) Se conecta a través de escritorio remoto al computador de la compañía,	6	14,63%
c) Recibe asesoría a través de escritorio remoto	5	12,20%
d) No requiere conectarse remotamente	16	39,02%
e) No requiere llevar información a su casa	9	21,95%
f) Lo trabaja en horario extendido en la compañía	23	56,10%
no sabe no responde	1	2,44%
Total encuestados		**41**

En la siguiente pregunta: ***10) En su computador de trabajo, ha sufrido incidentes como:*** la respuesta es múltiple con respecto a los incidentes ocurridos existe un promedio del 39.48% que afirma haber sufrido algún tipo de incidente y los incidentes más altos ocurridos son de mayor a menor lentitud en los procesos y discontinuidad en algunos aplicativos o servicios con el 58.54% y perdida de conexión con los aplicativos el 51,22%, seguido de ataques informáticos, como se indica en el cuadro No. 10.

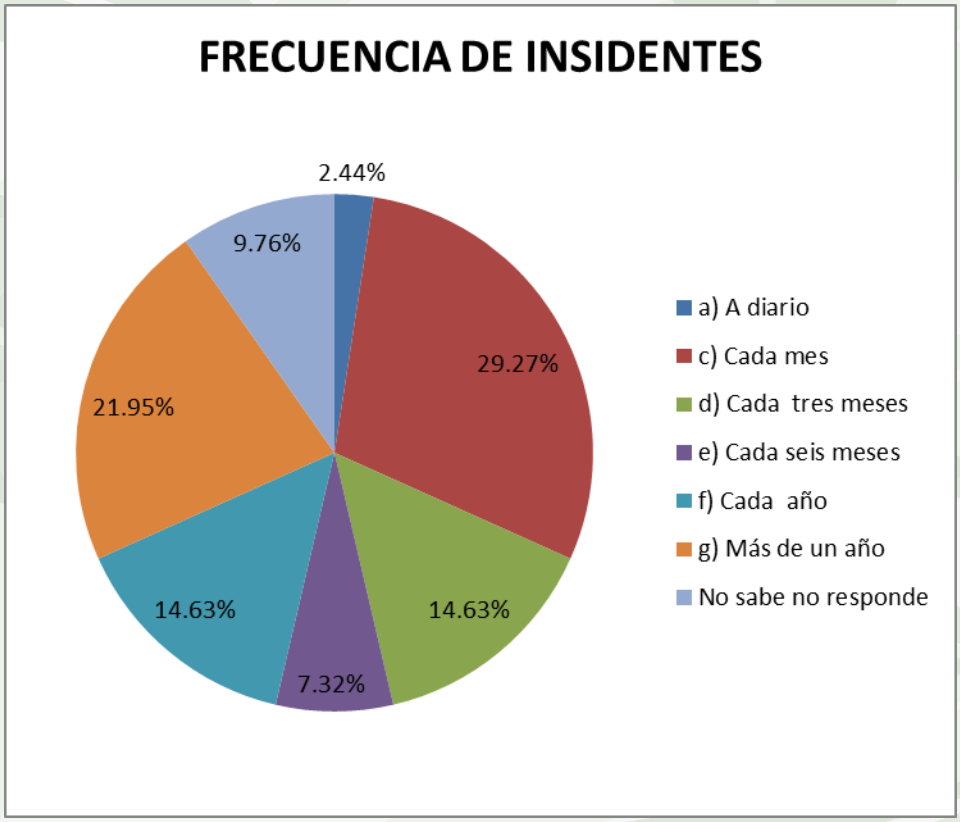
Cuadro No. 10: Incidentes.

10) En su computador de trabajo, ha sufrido incidentes como:	**Cantidad**	**Valor %**
a) Ataque de virus informáticos	18	43,90%
b) Perdida de información	7	17,07%
c) Lentitud en los procesos o aplicaciones	24	58,54%
d) Perdida de conexión con algún aplicativo	21	51,22%
e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, etc.	24	58,54%
f) Daño en su equipo de trabajo	3	7,32%
g) Ninguno de los anteriores	6	14,63%
Total Encuestados	**41**	

En cuanto a la pregunta**: *11) La frecuencia con que ha sucedido los incidentes en su equipo de trabajo es:*** como respuestas más significativa esta el 29.27% de frecuencia de incidentes ocurrida mensualmente seguida la del 21.95% ocurrida cada año, como se puede observar en el cuadro No. 11 y el grafico No. 4.

Cuadro No. 11: frecuencia de incidentes.

11) La frecuencia con que ha sucedido los incidentes en su equipo de trabajo es:	**Cantidad**	**Valor %**
a) A diario	1	2,44%
c) Cada mes	12	29,27%
d) Cada tres meses	6	14,63%
e) Cada seis meses	3	7,32%
f) Cada año	6	14,63%
g) Más de un año	9	21,95%
No sabe no responde	4	9,76%
Total general	41	100,00%



Grafica No. 4

Con la respuesta a esta pregunta ***12) ¿Qué tipo de aplicaciones corporativas o servicios maneja desde su computador ?,*** se puede identificar la existencia de 11 activos de información manejado por medios electrónicos y una consulta que llama la atención y representa el 29.27 % de los encuestados y se podría estar generando una amenaza a la integridad de la información contenida en las base de datos con el acceso mediante SQL a la base de datos, para lo cual debería hacerse mediante una aplicación propia del área a la cual pertenece la base de datos. Lo mismo sucede con la repuesta del literal n) acceso a escritorio remoto, para lo cual respondieron que lo utilizan el 60.98%, si este medio de acceso a la información no se encuentra bien configurado, se maneja contraseñas encriptadas y no se tiene establecido horarios de acceso, puede representar una amenaza para los activos de información como se indica en el cuadro No. 12.

Cuadro No. 12: Tipo de programas.

12) ¿Qué tipo de aplicaciones corporativas o servicios maneja desde su computador?	**Cantidad**	**Valor %**
a) Aplicación del área financiera	10	24,39%
b) Aplicación del área comercial (facturación)	19	46,34%
c) Aplicaciones de control de elementos específicos y técnicos de la compañía	6	14,63%
d) Aplicación de indicadores o cuadros de mando	16	39,02%
e) Aplicación de control documental	25	60,98%
f) Aplicaciones de comunicación	9	21,95%
g) Aplicación de control de atención al cliente	6	14,63%
h) Aplicación de nomina	2	4,88%
i) Aplicaciones de navegación en internet	26	63,41%
j) Herramienta de desarrollo	3	7,32%
k) Consulta directa a la base de datos mediante SQL server	12	29,27%
l) Aplicaciones para el control de proyectos y seguimiento de metas	5	12,20%
n) Aplicaciones de acceso a escritorio remoto	25	60,98%
Total respuestas		41

Para la pregunta: ***13) En el aplicativo que maneja tiene derecho a:*** en las respuestas se puede observar que el 31.71% de los usuarios encuestados tiene un perfil para realizar todas las actividades posibles en la aplicación, pero en la entrevista se confirma que ninguna persona realiza auditorias o seguimiento a este tipo de usuarios del sistema de información para verificar las actividades que realizan, los resultados se observan en el cuadro No. 13.

Cuadro No. 13: Roles de los usuarios

13) En el aplicativo que maneja tiene derecho a:	Cantidad	Valor %
a) Adicionar nuevos registros, b) Actualizar registros, c) Borrar registros, d) Consultar registros	13	31,71%
a) Adicionar nuevos registros, b) Actualizar registros, d) Consultar registros	6	14,63%
a) Adicionar nuevos registros, d) Consultar registros	3	7,32%
b) Actualizar registros	2	4,88%
b) Actualizar registros, d) Consultar registros	1	2,44%
d) Consultar registros	14	34,15%
no sabe no contesta	2	4,88%
Total	41	

Siguiendo con el análisis de la respuestas a la pregunta ***13),*** se observa que existen usuarios finales con permiso de borrar información lo cual representan el 17,07%, del total de los encuestados, esto puede representar una vulnerabilidad que amenaza la integridad de la información, si el administrador no realiza auditorias y las actividades realizadas por esos usuarios, además tiene permiso porque realmente lo necesitan o lo tiene por descuido de los administradores de las aplicaciones, el cuadro No. 14 indica esta precisión.

Cuadro No. 14: Roles a usuarios por su perfil

13) En el aplicativo que maneja tiene derecho a:	Cantidad	Valor %
a) Administrador	**8**	**19,51%**
a) Adicionar nuevos registros, b) Actualizar registros, c) Borrar registros, d) Consultar registros	5	**12,20%**
a) Adicionar nuevos registros, b) Actualizar registros, d) Consultar registros	2	**4,88%**
b) Actualizar registros	1	**2,44%**
b) Directivo	**3**	**7,32%**
d) Consultar registros	3	**7,32%**
d) Usuario Final Interno	**26**	**63,41%**
a) Adicionar nuevos registros, b) Actualizar registros, c) Borrar registros, d) Consultar registros	7	**17,07%**
a) Adicionar nuevos registros, b) Actualizar registros, d) Consultar registros	3	**7,32%**
a) Adicionar nuevos registros, d) Consultar registros	3	**7,32%**
b) Actualizar registros	1	**2,44%**
b) Actualizar registros, e) Consultar registros	1	**2,44%**
d) Consultar registros	11	**26,83%**
No sabe no responde	1	**2,44%**
f) Programador /desarrollador	**2**	**4,88%**
a) Adicionar nuevos registros, b) Actualizar registros, c) Borrar registros, d) Consultar registros	1	**2,44%**
a) Adicionar nuevos registros, b) Actualizar registros, d) Consultar registros	1	**2,44%**
No sabe no responde	**1**	**2,44%**
Total general	**39**	**95,12%**

Realizando un análisis a la respuesta de la pregunta ***14) ¿De qué programas / archivos hace copia de seguridad información?***, se puede decir que un buen porcentaje de los usuarios tiene claro los archivos que debe realizar copias, en cambio los usuarios finales hablan de documentos y archivos Excel que deben guardar respaldo, esto implica que existe información que se procesa fuera de las aplicaciones corporativas de la compañía; no obstante estos archivos pueden ser un control adicional a los aplicativos, el resultado se observa en el cuadro No. 15.

Cuadro No. 15: Copias de seguridad de la información

14) ¿De que programas / archivos hace copia de seguridad de la información?	**Cantidad**	**Valor %**
Archivos varios	8	19,51%
BBDD	3	7,32%
Datos empresariales	11	26,83%
Documentos	3	7,32%
Documentos, Excel	4	9,76%
Excel	3	7,32%
Informes	2	4,88%
No sabe no responde	7	17,07%
Total general	41	100,00%

La frecuencia con que se realiza las copias de seguridad de la información es muy importante para dar solución a un evento de contingencia y poder restaurar la continuidad del negocio, esto nos permite apreciar que solo el 9,76% de los encuestados realiza copias a diario, estos son administradores en un 80%; pero ante el conglomerado el de mayor porcentaje es del 26.83% que corresponde a frecuencia trimestral, que teniendo en cuenta la rutina del trabajo sería muy vulnerable y peligroso en caso de un evento catastrófico y tener que restaurar la información para impedir las continuidad del negocio, los valores porcentuales en función de la frecuencia se pueden observar cuadro No 16.

Cuadro No. 16.

15) ¿Con que frecuencia se saca copia?	**Cantidad**	**Valor %**
a) A diario	4	**9,76%**
b) Cada semana	5	**12,20%**
c) Cada mes	8	**19,51%**
d) Cada trimestre	11	**26,83%**
e) Cada semestre	7	**17,07%**
f) Cada año	2	**4,88%**
No sabe no responde	4	**9,76%**
Total general	**41**	**100%**

Por ultimo analizando las respuestas a la pregunta ***16) ¿Sobre qué programas /aplicaciones ha recibido capacitación?*** Se podría decir que la capitación se ha dirigido sobre el manejo de las aplicaciones corporativas, entre ellas la más alta capacitación 39.02% es a la administración documental y en un porcentaje del 12,20% afirma no haber recibido ninguna capitación, en promedio se ha recibido una capacitación del 15.52%, otro punto importante es que nadie menciona capacitación sobre cuidados, manejo de información, seguridad informática; tema descuidado en capacitaciones a los usuarios del sistema de información, por lo cual presenta vulnerabilidad y amenaza sobre los activos informáticos de la compañía, en conclusión la seguridad de la información es un tema que no se trata en las capacitaciones, que puede representar un alto riesgo y conllevar a daños en los activos de información de la compañía, el resultado de la encuesta en el cuadro No. 17.

Cuadro No. 17: Capacitaciones en las aplicaciones

16) ¿Sobre qué programas /aplicaciones ha recibido capacitación?	**Cantidad**	**Valor %**
Administración de Sistemas Técnicos	7	17,07%
Administración Documental	16	39,02%
Cuadros de mando	9	21,95%
Gestión de Calidad	6	14,63%
Manejo de equipo técnico vía remota	2	4,88%
Ninguno	5	12,20%
Office	2	4,88%
Sistema de Información Comercial	15	36,59%
Sistema financiero	6	14,63%
Software calculador de tarifas	1	2,44%
Todas las anteriores	1	2,44%
Total	41	15,52%

ANEXO No 4. ENCUESTA A USUARIOS DE LOS SISTEMAS INFORMATICOS

POR MEDIO DE LA PRESENTE SOLICITO SU AMABLE ATENCIÓN Y REALIZAR LA ENCUESTA, PARA EL DESARROLLO DEL PROYECTO TITULADO **"PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA"**

1) ¿Qué relación laboral tiene con la compañía?
- a) Contrato a término indefinido
- b) Contrato a término fijo
- c) Contrato de prestación de servicios
- d) Contrato a través de terceros
- e) Subcontratación *(Outsourcing*)

2) ¿Qué perfil tiene en los sistemas informáticos?
- a) Administrador
- b) Directivo
- c) Desarrollador o programador
- d) Soporte de aplicativo
- e) Usuario Final Interno
- f) Usuario Final Externo
- g) Programador /desarrollador
- h) Subcontrato

3) ¿Su computador en el trabajo es utilizado?
- a) Solo por usted
- b) Usted y su compañero de confianza
- c) Tres o más personas
- d) Con usuarios invitados o anónimos de vez en cuando.

4) ¿De los siguientes controles de seguridad informática cuales aplican a su trabajo?
- a) Control sobre el uso general del computador en el trabajo,
- b) Control para el uso de dispositivos de almacenamiento externo (memorias USB)
- c) Control para el manejo de claves de usuario
- d) Control para el uso de enlaces Inalámbricos
- e) Control para el uso del internet www
- f) Control para realizar copias de seguridad de la información
- g) Control en el uso del correo electrónico.
- h) Control para el cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales
- i) Control sobre el resguardo y protección de la información
- j) Control para el mantenimiento del computador
- k) Control para dar de baja un equipo de cómputo o periférico
- l) Control para modificar o cambiar configuraciones en el computador
- m) Medidas disciplinarias por incumplimiento de controles informáticos.

5) ¿En cuanto a la instalación de programas o aplicaciones?
- a) Lo Instala usted mismo
- b) Solicita asesoría al administrador de sistemas
- c) No necesita Instalar
- d) No lo ha intentado

6) ¿Para el manejo de contraseñas de su equipo y/o programas que tipo de combinación de Caracteres utilizas?
- a) Solo nombres conocidos
- b) Fechas conocidas
- c) Solo minúsculas
- d) Solo mayúsculas
- e) Combinación de mayúsculas y minúsculas
- f) Combinación de letras y números
- g) Combinación de todo tipo de caracteres

7) ¿Cuantos caracteres o letras utiliza para sus contraseñas?

a) Entre uno y tres
b) Entre cuatro y seis
c) Entre siete y nueve
d) Entre diez y doce
e) Más de doce caracteres

8) ¿Cuándo se ausenta temporalmente de la estación de trabajo, el computador?
a) Lo deja apagando
b) No lo apaga y se bloquea automáticamente
c) No lo apaga y lo deja bloqueando manualmente
d) No lo apaga y pocas veces lo deja bloqueando
e) No lo apaga ni lo bloquea
f) Solo se apaga cuando termina la jornada
g) Nunca se apaga

9) ¿Por labores propias de su desempeño en el trabajo de la compañía?
a) Procesa información fuera de la compañía
b) Se conecta a través de escritorio remoto al computador de la compañía
c) Recibe asesorías a través de escritorio remoto
d) No requiere conectarse remotamente.
e) No requiere llevar información a su casa
f) Lo trabaja en horario extendido en la compañía

10) En su computador de trabajo, ha sufrido incidentes como
a) Ataque de virus informáticos
b) Perdida de información
c) Lentitud en los procesos o aplicaciones
d) Perdida de conexión con algún aplicativo
e) Discontinuidad en algunos de los servicios corporativos (internet, aplicaciones, etc.)
f) Daño en su equipo de trabajo
g) Ninguno de los anteriores

11) La frecuencia con que ha sucedido los incidentes en su equipo de trabajo es:
a) A diario
b) Cada semana
c) Cada mes
d) Cada tres meses
e) Cada seis meses
f) Cada año
g) Más de un año

12) ¿Qué tipo de aplicaciones corporativas o servicios maneja desde su computador de trabajo?
a) Aplicación del área financiera
b) Aplicación del área comercial (facturación)
c) Aplicaciones de control de elementos específicos y técnicos de la compañía
d) Aplicación de indicadores o cuadros de mando
e) Aplicación de control documental
f) Aplicaciones de comunicación
g) Aplicación para el control de atención al cliente
h) Aplicación de nomina
i) Internet
j) Herramienta de desarrollo
k) Consulta directa a la base de datos mediante SQL server
l) Aplicaciones para el control de proyectos y seguimiento de metas
m) Aplicaciones especializadas para el control remoto de elementos específicos
n) Aplicaciones de acceso a escritorio remoto

13) En el aplicativo que maneja tiene derecho a:
a) Adicionar nuevos registros
b) Actualizar registros
c) Borrar registros

d) Consulta de registros

14) ¿De qué programas /archivos saca copia de seguridad de la información?
    a) _____
15) ¿Con que frecuencia se saca copia?
    a) A diario
    b) Cada semana
    c) Cada mes
    d) Cada trimestre
    e) Cada semestre
    f) Cada año
16) ¿Sobre qué programas /aplicaciones ha recibido capacitación?
    a) _____

ANEXO NO.5 ENTREVISTA ADMINISTRADORES

TEMARIO DE PREGUNTAS PARA ENTREVISTAR A LOS ADMINISTRADORES DE LOS SISTEMAS INFORMATICOS PARA EL PROYECTO: "PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA"
La encuesta será grabada con autorización del entrevistado y será utilizada solo para el análisis de información y desarrollo del proyecto propuesto, con el compromiso de que la información será de estricta confidencialidad y nada de lo que se diga será divulgado.
Además, una vez analizada la entrevista esta será borrada.

TEMARIO DE POSIBLES PREGUNTAS:

1) ¿Cuál es su cargo en la compañía?
2) ¿Cuál es su relación contractual con la compañía?
3) ¿Qué tipo de información maneja o administra en la compañía?
   a) ¿Quién es el directo responsable de la información que maneja?
   b) ¿La información que maneja en la aplicación la clasificaría como: sensible, personal, clasificada o publica?
   c) ¿Considera que la información administrada es imprescindible, para el normal desarrollo de la compañía?
   d) ¿Califique de 1 a 10 el valor de la información 1 mínimo valor, 10 valor máximo?
4) ¿Tienen implementado procedimientos escritos para realizar copias de respaldo?
5) ¿Tiene implementado procedimientos escritos de custodia de la información?
6) ¿Tiene implementado procedimientos escritos para la restauración de las copias de seguridad de la información?
7) ¿Han realizado pruebas de restauración de copias de seguridad información?
8) ¿Las aplicaciones que maneja o administra son de tipo: estándar o desarrollo a la medida?
   a) estándar
      i) ¿Existe servidor de pruebas para la aplicación antes de entrar en producción?
         (1) ¿Por qué no tienen servidor de pruebas?
      ii) ¿La aplicación está debidamente licenciada?
         (1) si
            (a) ¿Quién custodia el instalador de la aplicación y el documento de licenciamiento?
         (2) No
            (a) ¿Porque no está debidamente licenciada?
      iii) ¿Mediante qué medio brinda soporte el proveedor a la aplicación:
         (1) personalizado,
         (2) por medio de escritorio remoto
         (3) vía telefónica
         (4) chat?
   b) Desarrollo a la medida.
      i) ¿Existe servidor de pruebas para la aplicación en desarrollo antes de entrar en producción?
         (1) ¿Por qué no tienen servidor de pruebas?

ii) ¿Existe algún procedimiento para su aprobación y puesta en producción de las mejoras o desarrollo de la aplicación?
iii) ¿Qué controles de integridad, disponibilidad y confidencialidad tiene implementado en los procesos de la aplicación?
(a) ¿Quién custodia el instalador de la aplicación, el código fuente y los documentos de licenciamiento de la base de datos?
iv) ¿Hace cuánto se realizó la última actualización?
v) ¿Mediante qué medio brinda soporte el proveedor a la aplicación:
(1) personalizado,
(2) por medio de escritorio remoto
(3) vía telefónica
(4) chat?

9) ¿Cómo se resguarda el código fuente de la aplicación?
a) ¿Existe algún procedimiento para el manejo del código fuente y el código ejecutable de la aplicación?
b) ¿Existe servidor independiente para la base de datos o está en el mismo servidor de la aplicación?
c) ¿Usted mismo administra la base de datos?
10) ¿Quién gestiona la configuración del servidor?
11) ¿Qué políticas de seguridad informática de acceso a la información en la aplicación administrada tiene implementado?
a) ¿Cómo se gestiona la protección de información sensible?
b) ¿Cómo se gestionan los privilegios de acceso a la información de la aplicación?
c) ¿Qué procedimiento tiene implementado para la gestión de contraseñas?
d) ¿Tiene implementado horarios de acceso a la aplicación que maneja?
e) ¿Quién monitorea y revisa los derechos de acceso de los usuarios?
12) ¿Qué controles tiene implementado en la aplicación para salvaguardar la integridad disponibilidad y confidencialidad de la información?
a) ¿Existen usuarios con privilegios de administradores?
i) Si
(1) ¿Para qué actividades utiliza estos privilegios?
(2) ¿Hasta qué nivel de privilegios tiene?
ii) No
(1) ¿Por qué no existen más usuarios con este tipo de privilegios?
(2) ¿Los privilegios de administrador tiene clave compartida?
13) En cuanto al manejo de contraseñas para acceso al equipo y/o aplicaciones.
a) ¿Qué PSI tiene implementado?
b) ¿Cómo controla los privilegios?
c) ¿Cuál es el proceso de creación de contraseñas?
d) ¿Tiene algún procedimiento para los usuarios que han terminado su contrato, han sido suspendidos o han salido de vacaciones?
e) ¿El ingreso a la aplicación o información tienen establecidos horarios de ingreso?
f) ¿Cómo controlan los accesos a la aplicación en horarios extendidos?
g) ¿Cómo controlan las PSI implementadas?
14) ¿Existen usuarios que tengan acceso a aplicaciones a través de un programa de escritorio remoto por el internet?
a) ¿Qué tipo de programa utiliza?

b) ¿Cómo controlan este tipo de acceso?

15) ¿La aplicación que maneja sobre qué servicios utiliza sistemas encriptación
    a) Sobre las aplicaciones
    b) Las Comunicaciones
    c) Soporte de la información
    d) Sobre el correo electrónico
16) ¿Existe alguna aplicación / programa monitorear el acceso de usuarios a la aplicación durante las 24 horas del día y los 360 días del año?
    a) ¿Cómo se administran el monitoreo? y existe algún profesional encargado de analizar la información sensible de la base de datos.
17) ¿Llevan algún registro de auditoria sobre el ingreso de los usuarios directos e indirectos que ingresan a la aplicación o al sistema informático?
    a) ¿Un usuario directo o indirecto de su aplicación puede abrir varias sesiones sobre la misma aplicación en diferentes estaciones de trabajo?
18) ¿Cuándo un equipo requiere mantenimiento que procedimiento sigue?
19) ¿Usted conoce de los incidentes que han vulnerado la seguridad informática?
20) ¿En cuanto a los requisitos de usuarios / privilegios sobre la aplicación quien tiene control?
21) ¿Qué procedimientos / herramientas considera importantes

ANEXO No. 6 TEMARIO PARA ENTREVISTA ADMINISTRADOR DE RED.

TEMARIO DE PREGUNTAS PARA EL ADMINISTRADOR DE RED DE LOS SISTEMAS INFORMATICOS

La encuesta será grabada con autorización del entrevistado y será utilizada solo para el análisis de la información y desarrollo del proyecto propuesto, con el compromiso de que la información será de estricta confidencialidad y nada de lo que se diga será divulgado.

Además, una vez analizada la entrevista, ésta será borrada.

TEMARIO DE POSIBLES PREGUNTAS:

22) ¿Cuál es su cargo en la compañía?
23) ¿Cuál es su relación contractual con la compañía?
24) ¿Qué tipo de información maneja o administra en la compañía?
    a) ¿Quién es el directo responsable de la información que maneja?
    b) ¿La información que maneja en la aplicación la clasificaría como sensible, carácter personal, clasificada o publica?
    c) ¿Considera que la información administrada es imprescindible, para el normal desarrollo de la compañía?
    d) ¿Califique de 1 a 10 el valor de la información 1 no importante valor, 10 valor imprescindible?
25) ¿Tienen implementado procedimientos escritos para realizar copias de respaldo?
26) ¿Tiene implementado procedimiento escritos de custodia para la información?
27) ¿Tiene implementado procedimientos escritos para la restauración de las copias de seguridad de la información?
28) ¿Las aplicaciones que maneja o administra son de tipo: estándar o desarrollo a la medida?
    a) estándar
        i) ¿Existe servidor de pruebas para la aplicación antes de entrar en producción?
            (1) ¿Por qué no tienen servidor de pruebas?
        ii) ¿La aplicación está debidamente licenciada?
            (1) si
                (a) ¿Quién custodia el instalador de la aplicación y el documento de licenciamiento?
            (2) No
                (a) ¿Porque no está debidamente licenciada?
        iii) ¿Hace cuanto se realizó la última actualización?
        iv) ¿Mediante qué medio brinda soporte el proveedor a la aplicación:
            (1) personalizado,
            (2) por medio de escritorio remoto
            (3) vía telefónica
            (4) chat?
    b) Desarrollo a la medida.
        i) ¿Existe servidor de pruebas para la aplicación en desarrollo antes de entrar en producción?
            (1) ¿Por qué no tienen servidor de pruebas?
        ii) ¿Existe algún procedimiento para su aprobación y puesta en producción de las mejoras o desarrollo de la aplicación?

iii) ¿Qué controles de integridad, disponibilidad y confidencialidad tiene implementado en los procesos de la aplicación?
(a) ¿Quién custodia el instalador de la aplicación, el código fuente y los documentos de licenciamiento de la base de datos?

29) Existen usuarios que tengan acceso a la red y aplicaciones a través de programas de escritorio remoto utilizando la internet
a) ¿Cómo controlan el acceso?
b) ¿Qué aplicaciones utiliza para la comunicación remota?
c) ¿La aplicación está debidamente licenciada?
i) si
(1) ¿Quién maneja las licencias de la aplicación?
ii) No
(1) ¿Porque no tiene licencia?

30) ¿Cómo controlan que todos los computadores conectados en la compañía: sus programas, aplicaciones y sistemas operativos instalados estén debidamente licenciados?

31) ¿Existe un inventario de los activos informáticos?
a) ¿Existe algún procedimiento para el manejo del código fuente y el código ejecutable de las aplicaciones en desarrollo?
b) ¿Existe servidor independiente para la base de datos o está en el mismo servidor de la aplicación?

32) ¿Quién gestiona la configuración del servidor?

33) ¿Quién gestiona la configuración de los computadores de usuarios?

34) ¿Qué políticas de seguridad informática de acceso a la red tiene implementado?
a) ¿Cómo se gestiona la protección de la red?
b) ¿Cómo se gestionan los privilegios de acceso a la red?
c) ¿Qué procedimiento tiene implementado para la gestión de contraseñas?
d) ¿Tiene implementado horarios de acceso a las aplicaciones de la red?
e) ¿Quién monitorea y revisa los derechos de acceso de los usuarios?

35) ¿Cuentan con un servidor de comunicaciones?

36) ¿Tiene implementado zona desmilitarizada para los servidores en la red intranet?
a) ¿La zona desmilitarizada implementada esta mediante la Instalación de cortafuegos (firewall) o servidor de seguridad informática?
b) ¿La red se encuentra totalmente segmentada?
c) ¿Qué otros controles tiene implementado en la red para salvaguardar la integridad disponibilidad y confidencialidad de la información?
d) ¿Cualquier equipo puede ser conectado a la red de la compañía?
e) ¿Existen usuarios con privilegios de administradores?

37) ¿Tiene algún procedimiento para dar de baja a los usuarios que han terminado su contrato o han sido suspendidos
a) ¿Cuándo los usuarios salen de vacaciones qué medidas se toman con respecto a las sesiones de las aplicaciones?
b) ¿Cómo controlan las PSI implementadas?

38) ¿En qué servicios utiliza sistemas de encriptación
a) Sobre las aplicaciones
b) Las Comunicaciones
c) Soporte de la información bakup
d) En el correo electrónico

39) ¿Existe algún programa automatizado para monitorear la red durante las 24 horas y los 360 días?
    a) ¿Cómo lo administran? y existe algún profesional encargado de analizar la información
40) ¿Llevan algún registro o inventario de los usuarios directos e indirectos que ingresan a la red informática?
41) ¿Existe algún procedimiento de sanitización de equipo de cómputo dañados antes de dar de baja?
    a) ¿Qué hacen con los equipos dañados?
    b) ¿Para el mantenimiento de los equipos de cómputo, existe algún procedimiento?
    c) ¿Lo realiza personal interno de la compañía?
    d) ¿Existe contrato de prestación de servicios?
    e) ¿existe algún procedimiento de salvaguardar la confidencialidad de la información y los softwares instalados en el equipo?
42) ¿Cómo tienen implementado la seguridad de la información del equipamiento informáticos en
    a) ¿Servidores?,
    b) ¿Computadores de escritorio?
    c) ¿Portátiles?
    d) ¿Equipamientos de respaldo?
    e) ¿Periféricos?
    f) ¿Dispositivo de frontera?
    g) ¿Soportes de red?
43) ¿Tiene diseñado y documentado la topología de la red informática, identificando cada una de las tecnologías de comunicación y los controles de seguridad informática implementados?
44) ¿Existe presupuesto para invertir en seguridad informática?
45) ¿Con respecto a los años anteriores existe algún incremento en el presupuesto destinado a la seguridad informática?
46) ¿En que se invierten o centran los gastos de seguridad informática?
47) ¿Considera que es necesario diseñar o definir más presupuesto en los controles de seguridad Informática?
48) ¿Cuantos profesionales están dedicados a la gestión y control de la seguridad informática?
49) ¿Usted conoce de los incidentes que han vulnerado la seguridad informática?
50) ¿Qué otros procedimientos de buenas prácticas utilizan para mitigar los riesgos existentes en la compañía?
51) ¿Qué procedimientos /herramientas considera importantes para mejorar la seguridad informática?