RESUMEN – TRABAJO DE GRADO

AUTORES	**YEINNY YOHANA ACOSTA VERGEL** **VIANNY KARINA BUITRAGO SEPÚLVEDA** **LEIDY LISBETH CONTRERAS HERNÁNDEZ** **YORMAN JOSÉ MÁRQUEZ FUENTES**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**YESICA MARÍA PÉREZ PÉREZ**
TÍTULO DE LA TESIS	**FASE DE PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA DE SISTEMAS DE COMFAORIENTE EPS-S**

RESUMEN

(70 palabras aproximadamente)

EL DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA DE SISTEMAS DE COMFAORIENTE EPS-S, DESARROLLADO MEDIANTE UNA AUDITORIA PASIVA DEL NEGOCIO Y IDENTIFICACION DE RIESGOS Y/O AMENAZAS Y VULNERABILIDADES QUE ENFRENTA LA DEPENDENCIA, PERMITIRÁ LA ELABORACIÓN DEL DOCUMENTO FINAL ESTABLECIENDO LOS DOMINIOS Y OBJETIVOS DE CONTROL, SUSTENTADA, APLICADA, EL CUAL GARANTIZARÁ LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, QUE ES EL OBJETIVO FINAL DEL PRESENTE TRABAJO DE INVESTIGACIÓN.

CARACTERÍSTICAS

PÁGINAS: 200	PLANOS:	ILUSTRACIONES:	CD-ROM:

FASE DE PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA DE SISTEMAS DE COMFAORIENTE EPS-S

YEINNY YOHANA ACOSTA VERGEL
VIANNY KARINA BUITRAGO SEPÚLVEDA
LEIDY LISBETH CONTRERAS HERNÁNDEZ
YORMAN JOSÉ MÁRQUEZ FUENTES

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
ESPECIALIZACION AUDITORIA EN SISTEMAS
OCAÑA
2015

FASE DE PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA DE SISTEMAS DE COMFAORIENTE EPS-S

YEINNY YOHANA ACOSTA VERGEL
VIANNY KARINA BUITRAGO SEPÚLVEDA
LEIDY LISBETH CONTRERAS HERNÁNDEZ
YORMAN JOSÉ MÁRQUEZ FUENTES

Proyecto de grado presentado para optar al título de Especialistas en Auditoría de Sistemas

Directora
ING. YESICA MARÍA PÉREZ PÉREZ
Especialista en Auditoria de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
ESPECIALIZACION AUDITORIA EN SISTEMAS
OCAÑA
2015

DEDICATORIA

Dedico este nuevo logro en mi vida al ser que actúa en mi cada día "DIOS", por darme la fuerza, la constancia y sobre todo por mostrarme que quien trabaja con fé, dedicación y constancia puede alcanzar sus objetivos.

A mi madre ***TERESA HERNANDEZ HERNANDEZ*** *por su apoyo y ejemplo de mujer trabajadora y luchadora incansable, gracias a ti mamita estoy logrando mis objetivos propuestos.*

A mi padre ***ELISEO CONTRERAS CONTRERAS*** *por su amor y dedicación en todas las etapas de mi vida.*

A mis hermanos ***JOSE ELISEO CONTRERAS, OMAR FERNEY CONTRERAS Y JOSE MIGUEL BUITRAGO*** *por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida, pero sobre todo por ser ese motor que hace que logre mis objetivos convirtiéndome en una luchadora incansable pues lo que más anhelo es su felicidad.*

A mi compañero de vida ***JANUER ALBERTO MORENO PRADILLA*** *por su amor y apoyo incondicional en todas las metas que me propongo.*

Y demás familiares y amigos quienes han compartido conmigo en este camino y hoy ven esta meta cumplida. ¡Vamos por la Siguiente!

LEIDY LISBETH CONTRERAS HERNANDEZ

DEDICATORIA

Dedico este nuevo logro a Dios, por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más.
Gracias a esas personas importantes en mi vida, que siempre estuvieron listas para brindarme su apoyo. Con todo mi cariño les dedico esto a ustedes:
A mi madre ***OMAIRA SEPULVEDA TARAZONA*** *por su apoyo y sus grandes enseñanzas durante mi vida.*

A mi padre ***CARLOS ALIRIO BUITRAGO GRANADOS*** *por su amor y dedicación en todas las etapas de mi vida.*

A mis hermanos ***FABIAN ALIRIO BUITRAGO SEPULVEDA y KARLA STEFANY BUITRAGO SEPULVEDA*** *por compartir conmigo cada momento de mi vida.*

A ***EDGAR FABIÁN LABRADOR VALCARCEL*** *por su amor y apoyo incondicional en todas las metas que me propongo.*

VIANNY KARINA BUITRAGO SEPULVEDA

DEDICATORIA

Dedico esta meta alcanzada en mi vida a DIOS, por darme las fuerzas y perseverancia para llegar hasta acá y sobre todo por mostrarme que quien trabaja con empeño y dedicación se puede lo que se propone.

A mi madre ***ABELINDA VERGEL*** *por su apoyo incondicional, en todas las cosas que emprendo y darme el ser.*

A mi padre ***JUAN DE DIOS ACOSTA DELGADO*** *por su apoyo, y compañía en toda mi vida.*

A mi hermana ***LUISA FERNANDA ACOSTA VERGEL*** *por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida.*

Y demás familiares y amigos quienes han compartido conmigo en este logro que estoy culminando.

YEINNY YOHANA ACOSTA VERGEL

DEDICATORIA

Dedico esta meta que estoy a punto de culminar en mi vida a DIOS, por darme la sabiduría y perseverancia para llegar hasta acá y sobre todo por mostrarme que con esfuerzo y con dedicación se consigue lo que se propone.

A mi madre ***LUZ MARINA FUENTES*** *por su apoyo siempre, en todas las actividades que emprendo.*

A mi padre ***JOSE ANTONIO MARQUEZ*** *por su apoyo incondicional siempre.*

A mis hermanos ***LINA Y CRISTIAN MARQUEZ*** *por apoyarme incondicionalmente y compartir conmigo cada día.*

Y demás familiares y amigos quienes han compartido conmigo en este logro que estoy culminando.

YORMAN JOSE MARQUEZ FUENTES

AGRADECIMIENTOS

*Agradecemos a **"DIOS"** ser supremo y creador de todas las cosas, por darnos la inteligencia, sabiduría y Constancia para lograr cada meta propuesta.*

*A la Ingeniera **YESICA MARIA PEREZ PEREZ** por el tiempo, orientación y aportes que nos brindó para consolidar este nuevo logro.*

Y a todas aquellas personas que lograron orientarnos y motivaron para el desarrollo de ésta especialización.

CONTENIDO

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCION

En el presente documento se presenta el diseño de la fase de planeación de un sistema de gestión de seguridad de la información para la dependencia de sistemas de COMFAORIENTE EPS-S.

Esta propuesta tiene como finalidad aportar a la organización a mejorar la calidad de los controles informáticos, a dejar sentados los elementos conceptuales y teóricos que les permitan a las personas que allí laboran tomar las decisiones correctas para utilizar adecuadamente la tecnología y contribuir a disminuir los niveles de inseguridad de la información en la organización.

Consciente de las necesidades actuales que presenta la dependencia de sistemas de COMFAORIENTE EPS-S, con respecto a la seguridad de la información, se realiza la fase de planeación de un sistema de gestión se seguridad de la información, como herramienta que le permita consolidar una estrategia para evitar afectaciones en la disponibilidad, integridad y confidencialidad de la información.

Del mismo modo busca orientar como los riesgos de la seguridad de la información deben ser conocidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzca en la tecnología y en los procesos de la organización.

1. FASE DE PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DEPENDENCIA DE SISTEMAS DE COMFAORIENTE EPS-S

1.1. PLANTEAMIENTO DEL PROBLEMA

A nivel mundial se observan eventos que generan urgencia en la necesidad de tener mayor seguridad en la protección de la información.

Se ha evidenciado que la mayoría de las empresas han reforzado las medidas de seguridad pero nunca se sabe cómo y cuándo pueden estar expuestas a posibles ataques.

Con el fin de brindar protección empresarial se requiere de un sistema de seguridad de la información que indique como sobrevivir a los múltiples escenarios, preparando a las empresas en el manejo de amenazas inesperadas que podrían afectar a futuro.

En el ámbito regional se evidencia que muchas empresas son grandes en infraestructura y en clientes, sin embargo no invierten en seguridad de la información, tal vez, porque creen que están exentas de sufrir situaciones inesperadas que comprometan la información y los activos asociados a ella, ocasionando a largo plazo pérdidas económicas en incluso sanciones legales.

COMFAORIENTE EPS-S es una empresa que maneja información de 118.000 afiliados en 15 municipios del departamento Norte de Santander, ésta debe ser protegida, preservada y conservada de manera segura, ya que es consultada diariamente por la red contratada para la prestación de servicios de salud de todos sus usuarios.

Es importante mencionar que la salud es un deber del estado con toda la población por ende las Empresas Promotoras de Salud son quienes administran los recursos para la prestación de servicios, del mismo modo como administran recursos económicos son las responsables de la información de cada uno de sus afiliados.

1.2. FORMULACIÓN DE LA PREGUNTA DE INVESTIGACIÓN

¿El diseño de la fase de planeación del sistema de gestión de seguridad de la información para la dependencia de sistemas de Comfaoriente EPS-S será un instrumento inicial adecuado a las necesidades de aseguramiento de la información y los activos asociados en la dependencia de Sistemas de COMFAORIENTE EPS-S?

1.3. OBJETIVOS

1.3.1. Objetivo General

Planear el sistema de gestión de seguridad de la información para la dependencia de sistemas de COMFAORIENTE EPS-S.

1.3.2. Objetivos Específicos

- Realizar un diagnóstico de la seguridad de la información en la dependencia de sistemas de Comfaoriente EPS-S por medio de una auditoria pasiva utilizando la NTC/ISO 27001:2013

- Identificar los riesgos que exponen la seguridad de la información de la dependencia de sistemas de Comfaoriente EPS-S.

- Documentar los parámetros y el desarrollo de la planeación del sistema de gestión de seguridad de la información (SGSI) en la dependencia de sistemas de Comfaoriente EPS-S.

1.4. JUSTIFICACIÓN

En una Empresa Promotora de Salud la prestación de servicios debe ser eficiente, las operaciones deben estar basadas en tecnología y sistemas de información donde se manejan grandes cantidades de información la cual debe estar disponible de forma confiable e integra para ser consultada por los actores de la red prestadora contratada y de sus afiliados. La planeación de un sistema de gestión de seguridad de la información dará apoyo al mejoramiento continuo una de las políticas de seguridad de COMFAORIENTE EPS-S permitiendo resguardar los activos y la información de la misma, la cual es de vital importancia pues está directamente relacionada con la prestación de servicios de Salud a sus 115.000 afiliados en todo el departamento través de la red prestadora contratada COMFAORIENTE EPS-S está vigilada por la Superintendencia Nacional de salud, el Ministerio de Salud y la Protección Social y los entes de control, de éste modo cualquier irregularidad con el manejo de la información ocasionaría a sanciones.

De este modo se hace necesaria la elaboración de un PLAN DE GESTION DE SEGURIDAD DE LA INFORMACION en la dependencia de sistemas de COMFAORIENTE EPS-S que garantice la Integridad, la disponibilidad y la confidencialidad de la información de sus afiliados.

1.5 HIPÓTESIS

Un documento donde se evidencie el diseño de un plan de Gestión de seguridad de la información basado en la Norma ISO 27001:2013 para la dependencia de sistemas de COMFAORIENTE EPS- S será considerado como eje fundamental para el uso de la información que contribuya al cumplimento de los objetivos misionales de la misma.

1.6 DELIMITACIONES

1.6.1 Geográfica

Dependencia de Sistemas de COMFAORIENTE EPS-S sede Administrativa, Cúcuta.

1.6.2 Delimitación Conceptual

Para la realización de ésta Investigación se tendrá en cuenta los siguientes conceptos: Políticas de Seguridad de la información, Sistemas de Gestión de Seguridad, Gestión de Riesgos, vulnerabilidad, disponibilidad, integridad, confidencialidad, sistemas de Identificación, prestación de Servicios.

1.6.3 Delimitación Temporal

La duración de ésta investigación será de tres (3) meses, a partir de la aprobación del anteproyecto

2. MARCO REFERENCIAL

2.1. MARCO HISTÓRICO

La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros. Para este proyecto se consideran activos de información los mencionados anteriormente. Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades.

2.1.1. Antecedentes. En el año 2004 se publicó la UNE 71502 titulada Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002.

Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001.

Arean Hernando Velasco Melo4, escribió en el 2008 un artículo sobre "el derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001". Este artículo pretende informar sobre la existencia y diversas modalidades que incluye el Derecho informático y crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad. La metodología empleada para explicar las diversas áreas de impacto es la seguida por la norma ISO 27001 en el dominio que hace referencia al cumplimiento y que comprende: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual, y el tratamiento de los incidentes informáticos.

2.2. MARCO CONTEXTUAL

2.2.1. La Organización. La Caja de Compensación Familiar del Oriente Colombiano es una Corporación de derecho privado sin ánimo de lucro, hace parte del Sistema de Compensación Familiar, regido por la Ley 21 de 1982 y las normas que la complementan, con personería jurídica otorgada por la Gobernación de Norte de Santander, mediante Resolución N° 0083 del 26 de junio de 1968.

El área de influencia por disposición de la Ley es el Departamento Norte de Santander, posee una sede principal en la ciudad de Cúcuta y dos seccionales localizadas en Ocaña y Pamplona y una Oficina en Tibú. La Seccional Ocaña, tiene jurisdicción en los municipios de Abrego, Convención, Cáchira, Hacarí, El Tarra, La Esperanza, La Playa, Ocaña y San Calixto; la Seccional Pamplona, atiende los municipios de Bochalema, Cácota, Chitagá, Durania, Labateca, Pamplona, Pamplonita, Mutiscua, Toledo y Silos y la Sede Administrativa Cúcuta atiende los demás municipios del Departamento.

En el Régimen Subsidiado en Salud, Mediante Resolución Nº 1396 de diciembre 4 de 1996 COMFAORIENTE recibió autorización del Ministerio de Salud, hoy Ministerio de la Protección Social, para administrar los recursos del Régimen Subsidiado en Salud, con el objeto de garantizar la Prestación del Plan Obligatorio de Salud Subsidiado POS-S en la zona geográfica de su influencia. Esta autorización incluyó el deber de inscripción y afiliación, la garantía de la cobertura de riesgos y servicios a que tienen derecho los afiliados al régimen subsidiado, de acuerdo con el Plan de Beneficios contenidos en el Capítulo III del Acuerdo 23 de 1995 del CNSSS, demás normas que lo modifiquen, aclaren o adicionen y las señaladas en el artículo 10º del Decreto 2357 de 1995; actualmente, la EPS-S opera en 15 municipios, en los cuales posee oficina de atención al afiliado y una red prestadora de servicios que cubre toda el área de influencia

2.2.2. Dependencia de la organización. El desarrollo de la investigación se llevara a cabo para el área de Sistemas de Comfaoriente EPS_S en la ciudad de Cúcuta de norte de Santander Colombia, donde se estudiará y se diseñará un plan de gestión de seguridad de la información para la administración de TI en Comfaoriente EPS-S.

2.3. MARCO TEORICO

2.3.1 ISO/IEC 27001:2005

Publicada el 15 de Octubre de 2005, es la norma principal de la familia de la ISO27000[1], y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no

[1] INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000. www.iso27000.es. 2008

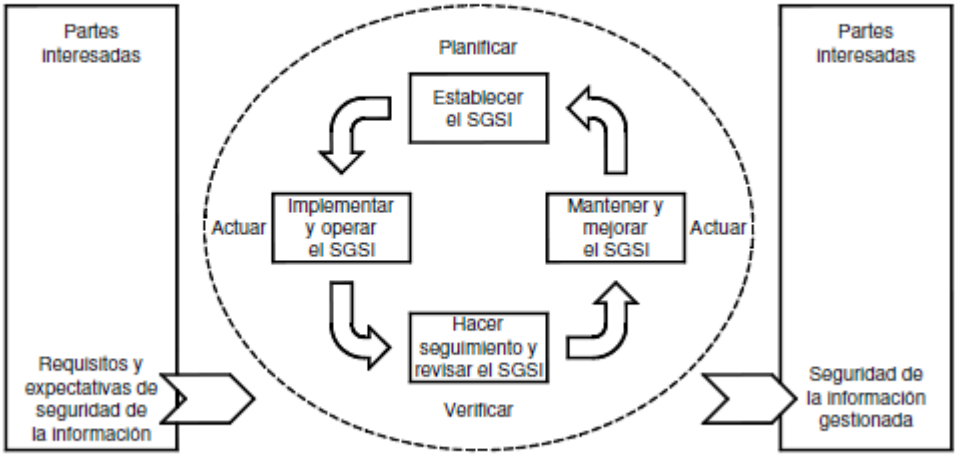
aplicabilidad de los controles no implementados. Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI.

2.3.2. ISO/IEC 27001:2013

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas. Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La Figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. La Figura 1. [2]

Figura 1.Modelo PVHA aplicado a los procesos SGSI



Fuente: norma técnica colombiana NTC- ISO/IEC 27001

[2] Norma técnica Colombiana NTC-ISO/IEC 27001

2.3.2. ISO/IEC 27002:2005

Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, mencionados en el anexo A de la ISO 27001, 39 objetivos de control y 133 controles.
Los dominios a tratar son los siguientes:

- **Políticas de Seguridad:** Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

- **Organización de la seguridad de la información:** Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

- **Gestión de activos:** Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

- **Seguridad de los recursos humanos:** Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

- **Seguridad física y ambiental:** Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

- **Gestión de comunicaciones y operaciones:** Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

- **Control de accesos:** El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

- **Sistemas de información, adquisición, desarrollo y mantenimiento:** Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

- **Gestión de incidentes de seguridad de la información:** Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de

administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

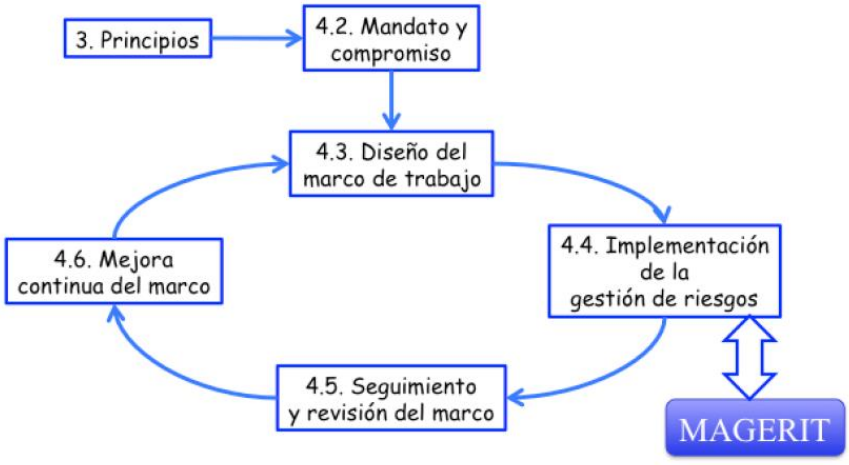
- **Gestión de continuidad del negocio:** Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

- **Cumplimiento:** Busca que las empresa cumpla estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

2.3.3. Magerit

Siguiendo la terminología de la normativa ISO 31000, Magerit[3] responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 2.Magerit



Fuente: Magerit- versión 3.0 metodología de análisis y gestión de riesgos de los sistemas de información libro I- Método

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC:

[3] **Magerit- versión 3.0 metodología de análisis y gestión de riesgos de los sistemas de información libro I- Método**

Guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. Magerit persigue los siguientes objetivos:

Directos:

1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos
4. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Declaración de aplicabilidad

Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

Cumplimiento de normativa

Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

Plan de seguridad

Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

2.4. MARCO CONCEPTUAL

2.4.1. Amenaza

Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

2.4.2. Apropiación

Las apropiaciones son autorizaciones máximas de gasto que el Congreso de la República aprueba para ser comprometidas durante la vigencia fiscal respectiva. Después del 31 de Diciembre de cada año estas autorizaciones expiran y en consecuencia no podrán comprometerse, adicionarse, transferirse.

2.4.3. Auditoría

Puede definirse como el proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

Otro concepto de auditoría definido por Echenique es, "un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia de una sección o un organismo y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos. El encargado de realizar las auditorias es el auditor, un auditor es la persona que evalúa la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación".

2.4.4. Auditoría Informática

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientes los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicional de la auditoría.

2.4.5. Control

Cualquier medido que tome la dirección, el Consejo y otros, para mejorar la gestión de riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas.

2.4.6 Control interno

Todas las medidas utilizadas por una empresa para protegerse contra errores, desperdicios o fraudes y para asegurar la confiabilidad de los datos. Está diseñado para ayudar a la operación eficiente de una empresa y para asegurar el cumplimiento de las políticas de la empresa.

2.4.7 Control Interno Informático

Sistemas Integral al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

2.4.8 Disponibilidad

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

2.4.9 Evaluación del riesgo

Proceso global de estimar la magnitud de los riesgos y decidir si un riesgo es o no tolerable.

2.4.10. Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

2.4.11. Identificación del peligro

Proceso que permite reconocer que un peligro existe y que a la vez permite definir sus características.

2.4.12. Identificación del riesgo

Proceso para determinar lo que puede suceder, por qué y cómo.

2.4.13. ISO (Organización Internacional de Normalización)

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

2.4.14. Riesgo

Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

2.4.15. Tratamiento del riesgo

Selección e implementación de las opciones apropiadas para ocuparse del riesgo.

2.4.16. Valoración del riesgo

Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

2.4.17. Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

2.5. MARCO LEGAL

En Colombia han sido diversos los esfuerzos por regular la actividad de TI, sin embargo, el dinamismo del sector casi siempre está varios pasos adelantes de la legislación. El proceso sobre el diseño un plan de gestión de seguridad de la información para la dependencia de sistemas de Comfaoriente EPS-S que se piensa desarrollar se considera un conjunto compuesto por leyes y normas nacionales, junto con estándares de referencias internacionales.

Entre los elementos Nacionales se tiene:

2.5.1. Marco Normativo General

- Ley 1341 de 2009, también conocida como Ley TIC
- Resolución 2060 de 2009. Plan de Emergencia y Contingencias del Sector de las Telecomunicaciones

2.5.2. Educación

- Resolución 3462 de 2003. Formación profesional en IT
- Ley 029 de 1990. Fomento de la investigación
- Ley 1286 de 2009. Ley Ciencia y Tecnología

2.5.3. Acceso y Uso de TI- Ecosistema Digital

- Artículo 11 del Proyecto de Ley 124/10C. Privilegio al acceso a Internet

2.5.4. El análisis de riesgos

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso de 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. En el Capítulo II, Principios Básicos, se dice: Artículo 6. Gestión de la seguridad basada en los riesgos. 1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. 2. 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, 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.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, se dice: Artículo 13. Análisis y gestión de los riesgos. 1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos. 2. 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. 3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que en su Artículo 1, Objeto de la Ley, dice así: 28 Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias. La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su

artículo 9 (Seguridad de los datos) dice así: El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2.5.5. **Ley 603 de 2000**

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

2.5.6. El derecho de autor.

Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley". Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino. Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia. Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. Decreto 1360 de 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor". Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

2.5.7. Norma Técnica Colombiana NTC-ISO/IEC 27000

Norma Técnica Colombiana NTC-ISO/IEC 27000 Evaluación y tratamiento del riesgo Evaluación de los riesgos de seguridad

3. DISEÑO METODOLOGICO

3.1. TIPO DE INVESTIGACIÓN

Actualmente se llevara a cabo el desarrollo del proyecto como una investigación descriptiva permitiendo comprobar todas las características de la solución del problema planteado en la organización que se está realizando dicho estudio en este caso el área de sistemas de Comfaoriente EPS-S, además tendrá un enfoque cuantitativo ya que se aplican métodos de recolección de información, con esto se aspira visualizar el diseño de un Sistema de Gestión de la Seguridad de la Información, y así ayudar a mejorar la gestión de los riesgos asociados con la información. En síntesis la investigación tendrá un enfoque descriptivo, permitiendo comprobar sistemática y progresivamente las características de la solución al problema planteado en la empresa objeto de estudio.

3.2. POBLACIÓN Y MUESTRA

Actualmente la dependencia de sistemas de COMFAORIENTE EPS-S cuenta con una población pequeña y debido a esta, se decidió que la muestra seria el total de la población conformada por los integrantes de la dependencia de sistemas de COMFAORIENTE EPS-S, Jefe de Sistemas, Desarrollador y un Técnico.

3.3. TÉCNICAS DE RECOLECCIÓN DE DATOS

Durante el desarrollo de este proyecto se utilizarán fuentes primarias y secundarias de recolección de información, utilizadas para la identificación o determinación de que controles o aspectos de las diferentes Normas y estándares que se ampliaran al área de sistemas de Comfaoriente EPS-S

Entre las fuentes primarias de información utilizadas en el estudio investigativo descriptivo se encuentran la asesoría de ingenieros de sistemas y especialistas, docentes de la Universidad Francisco de Paula Santander Seccional Ocaña que provean información base para este estudio; se utilizará la encuesta a los empleados del área objeto de estudio(dependencia de sistemas de Comfaoriente EPS-S); todo esto con el fin de conocer a fondo las operaciones de la sección para obtener una visión clara de los procedimientos realizados en la misma. En este estudio se emplearán diferentes instrumentos de recolección de información como: la encuesta y observación directa. (Ver anexo A)

Fuentes Secundarias: Entre las fuentes secundarias de información se cuenta con la información extraída de revistas, libros y textos de clase, documentación, bibliotecas y consultas virtuales.

4. PRESENTACION DE RESULTADOS

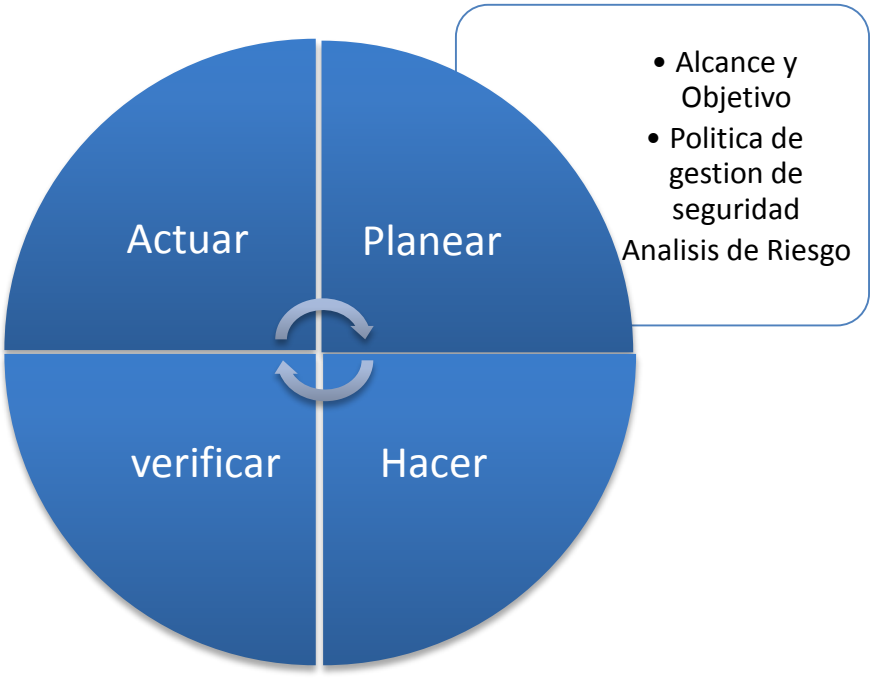
Para el logro de los objetivos propuestos se implementaron una serie de actividades(cuadro 1) que permiten identificar resultados evidenciado los riegos que enfrenta la Dependencia del área de sistemas de Comfaoriente EPS-S. Sin embargo Siguiendo la Metodología PVHA en la cual está divido en diferentes fases y en la cual nos centramos en la fase de planear (ver figura 3).

Cuadro 1. Actividades

OBJETIVOS	ACTIVIDADES
Realizar un diagnóstico de la seguridad de la información en la dependencia de sistemas de Comfaoriente EPS-S por medio de una auditoria pasiva utilizando la NTC/ISO 27001:2013	1. Recopilar y ajustar la información de la empresa como: misión, visión, objetivos, procesos entre otros. 2. Diseñar y Aplicar instrumentos (Lista de Chequeo, Encuesta, entrevista, papeles de trabajo.) de recolección de información. 3. Diseño de programa de auditoria, plan de auditoria y redacción de informe luego de llevar a cabo la auditoria.
Identificar los riesgos que exponen la seguridad de la información de la dependencia de sistemas de Comfaoriente EPS-S.	4. Diseñar herramientas para la identificación de riesgos (matriz,...) 5. Aplicación de las herramientas de identificación de riesgos
Documentar los parámetros que guiaran la planeación del sistema de gestión de seguridad de la información (SGSI) en la dependencia de sistemas de Comfaoriente EPS-S.	1. Identificación de alcances y objetivos. 2. Crear una política de gestión de seguridad basada en la norma ISO 27001:2013.

Fuente: autores del proyecto LKYY

Figura 3.Metodología PVHA



Fuente: Adecuación por autores del Proyecto LKYY

4.1. Realizar un diagnóstico de la seguridad de la información en la dependencia de sistemas de Comfaoriente EPS-S por medio de una auditoria pasiva utilizando la NTC/ISO 27001:2013.

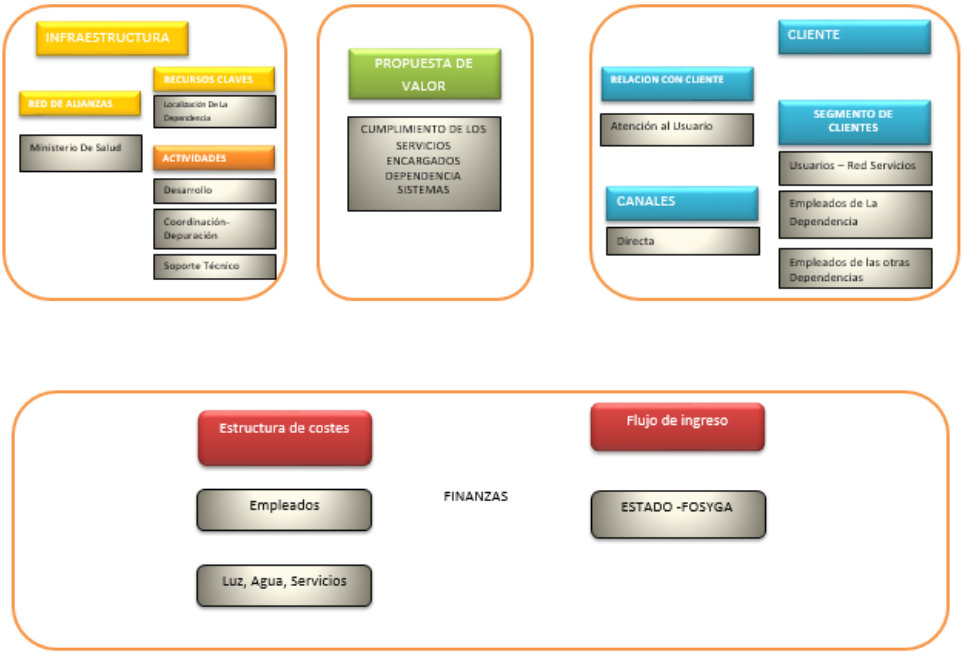
4.1.1 Modelado del negocio

En el desarrollo del modelo del negocio de la Dependencia nos basamos, en el de Alexander Osterwalder[4], el cual describe de manera lógica la forma en que las organizaciones crean, entregan y capturan valor. El proceso del diseño del modelo de negocios es parte de la estrategia de negocios, por lo que es de vital importancia estructurar este tipo de recursos para conocer a profundidad cómo opera una empresa y conocer las fortalezas y debilidades de la misma.

Cabe mencionar que todo modelo de negocios aportará un valor agregado a cualquier empresa que haga uso de ellos, pues a partir de los mismos, existirá una mayor noción y visión de la organización, a través de un enfoque sistémico que englobe todos los aspectos de la corporación.

[4] http://www.assaabloy.cl/uploads/Canvas_de_Osterwalder.pdf

Figura 4.Modelo del Negocio



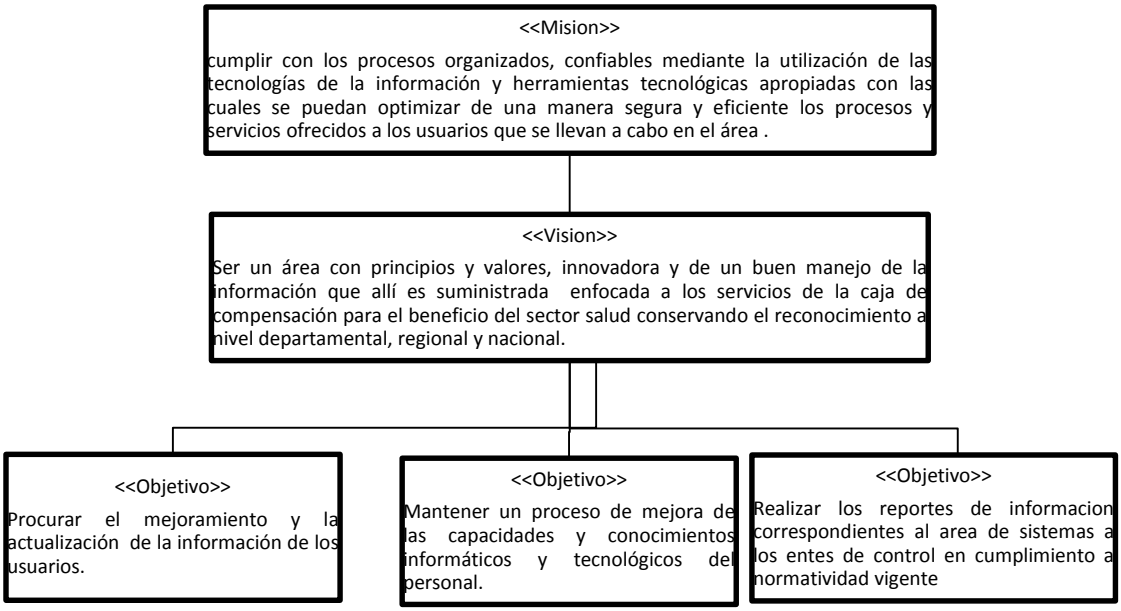
Fuente: Autores del Proyecto LKYY

4.1.2 Propuesta Objetivos de la dependencia

La dependencia de sistemas de Comfaoriente EPS no cuenta con Misión, Visión, objetivos y estructura organizacional definida por lo tanto se presenta la siguiente propuesta con base en los objetivos de calidad de la Caja de Compensación del Oriente Colombiano COMFAORIENTE. Siguiendo el formato En el anexo 8 y 9 el cual se empleó para hacer la evaluación de las propuestas y se evidencia el cumplimientos de las características de calidad definidas por **l**a misión y visión, tomando como definiciones de Misión por parte de Philip Kotler y Gary Armstrong (Marketing, 2004) como "un importante elemento de la planificación estratégica**"** porque es a partir de ésta que se formulan objetivos detallados que son los que guiarán a la empresa u organización**.** Por su parte O. C. Ferrel y Geoffrey Hirt, autores del libro "Introducción a los Negocios en un Mundo Cambiante" (McGraw Hill, 2004), la misión de una organización "es su propósito general"**.** Responde a la pregunta ¿qué se supone que hace la organización?"; podría considerarse también que la misión "enuncia a que clientes sirve, que necesidades satisface y qué tipos de productos ofrece. Por su parte, una declaración de misión indica, en términos generales, los límites de las actividades de la organización".[5] Por otra parte la Visión, tal como lo define Fleitman Jack en su obra "Negocios Exitosos" (McGraw Hill, 2000) viene a ser "el camino al cual se dirige la empresa a largo plazo y sirve de rumbo y aliciente para orientar las decisiones estratégicas de crecimiento junto a las de competitividad

[5] (2) Fundamentos de Marketing, Stanton, Etzel y Walker, 13a Edición, Editorial McGraw Hill, 2004, Pág. 668.

Figura 5.Misión- Visión- Objetivos



Fuente. Autores del Proyecto LKYY

A través del análisis hecho después de la auditoría realizada y tomando de partida el anexo 3 donde utilizamos unos formatos para definir una propuesta tanto para la misión y visión de la dependencia, se pudo sintetizar los siguientes objetivos que debe cumplir la dependencia de sistemas de Comfaoriente EPS-S:

- Procurar el mejoramiento y la actualización de la información de los usuarios.
- Mantener un proceso de mejora de las capacidades y conocimientos informáticos y tecnológicos del personal.
- Realizar los reportes de información correspondientes al área de sistemas a los entes de
- control en cumplimiento a normatividad vigente.

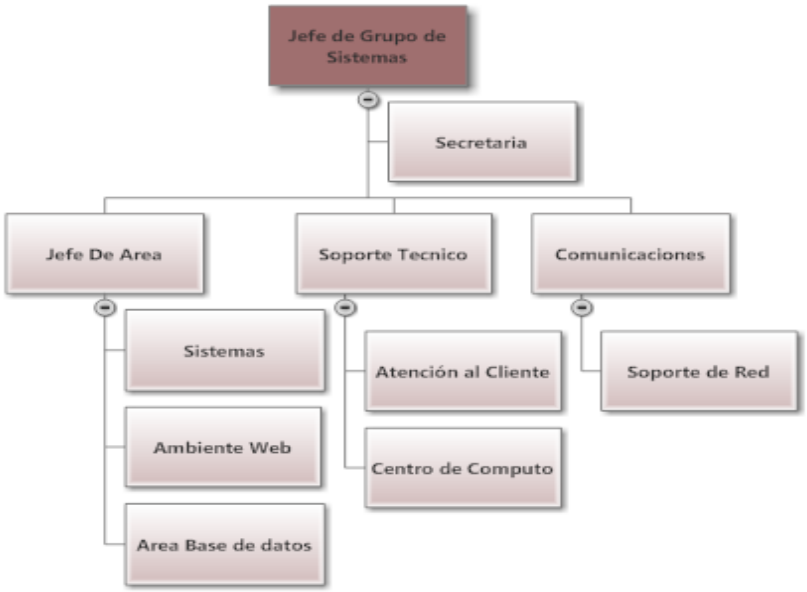
4.1.3. Propuesta estructura Orgánica

Se plantea una estructura orgánica para la dependencia de sistemas de COMFAORIENTE EPS-S, debido a que al momento de la recolección de información se pudo evidenciar que no se contaba con dicha estructura establecida.

La estructura Orgánica planteada para la dependencia de Sistema de COMFAORIENTE cuenta con los niveles jerárquicos necesarios para el correcto desempeño de las funciones de la misma, un Jefe de Grupo de sistemas, el cual posee el apoyo de una secretaria para el

manejo de documentación y a su vez dirige tres secciones jefe de área de sistemas, soporte técnico y Desarrollador.

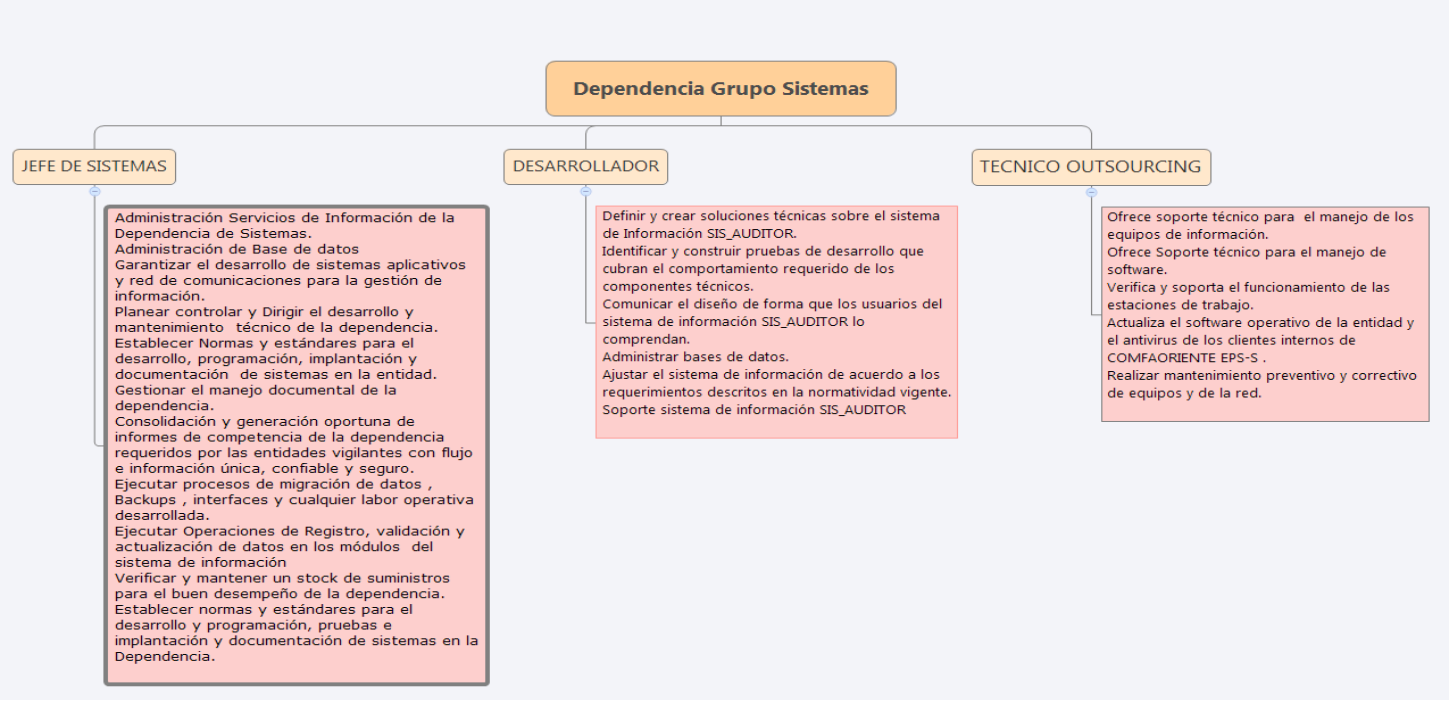
Figura 6.Estructura orgánica de la Dependencia del área de Sistemas de Comfaoriente EPS-S



Fuente. Autores del Proyecto LKYY

En la figura 6 Se plantea para la dependencia responsabilidades que cumplen el personal y que no se encuentran plasmadas en documentos para dejar una constancia de aquellas funciones acarrea ciertos cargos de la dependencia.

Figura 7.Responsabilidades de la dependencia de Sistema

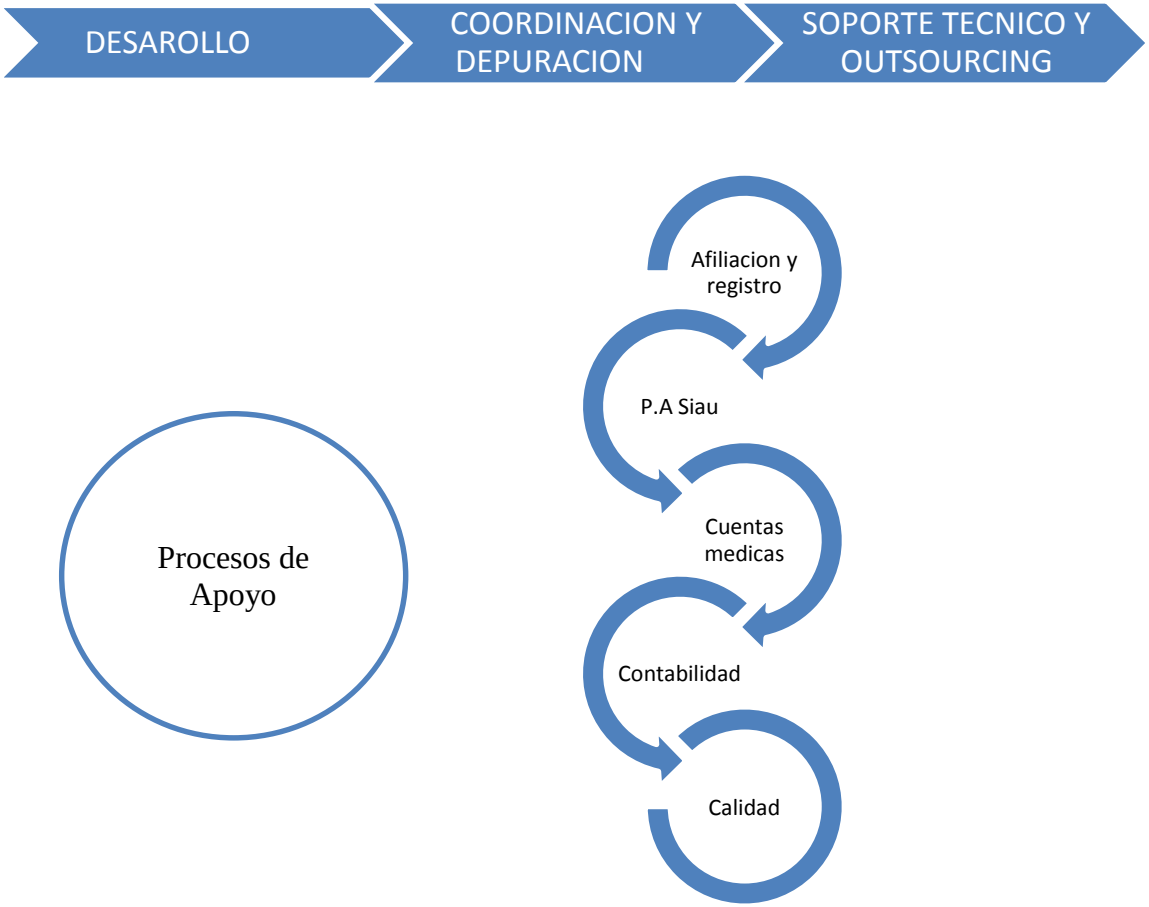


Fuente: Autores del proyecto LKYY

4.1.4 Cadena de Valor de la dependencia del área de sistemas

La dependencia del área de sistemas tiene dos procesos fundamentales: que son desarrollo o mejoras de aplicativos y soporte Outsourcing, para llevar a cabo un buen resultado en sus procesos la dependencia tiene 5 de apoyo donde suministran información, y obtienen el respaldo necesario, de esta forma consolidando un resultado que apoya el logro de sus objetivos.

Figura 8.Cadena de valor de la dependencia del área de sistemas de Comfaoriente EPS-S

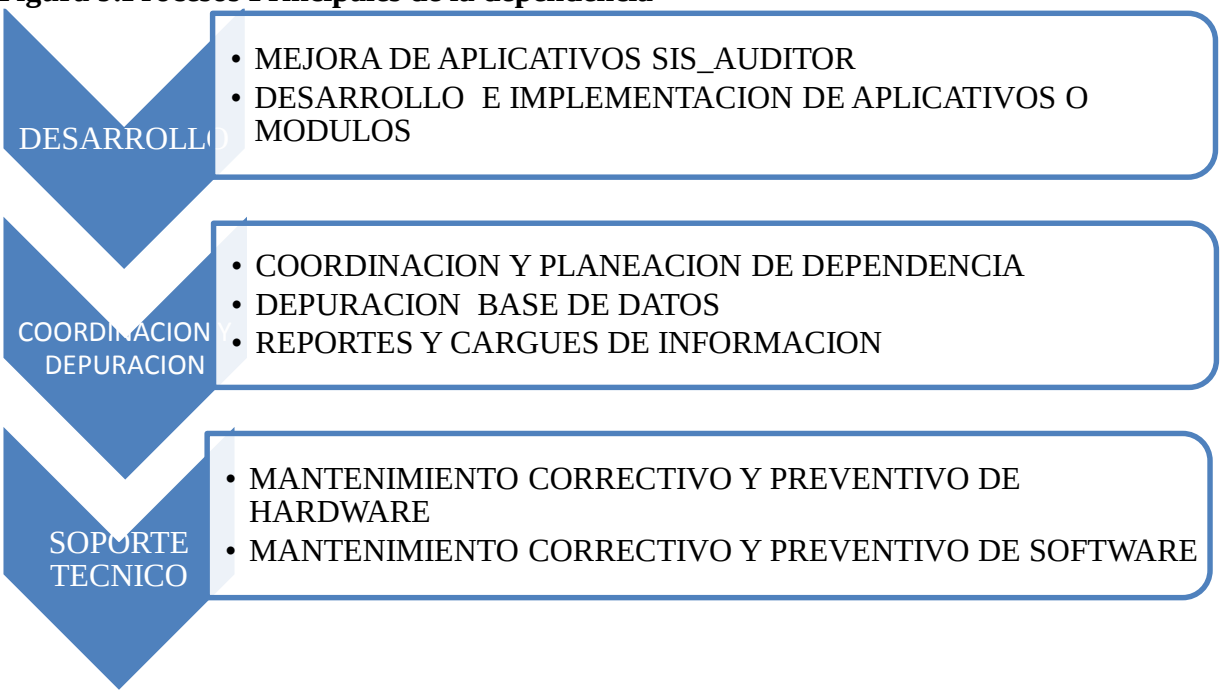


Fuente: Autores del Proyecto LKYY

4.1.5. Procesos de la Dependencia del área de sistemas de Comfaoriente EPS-S

La dependencia del área de sistemas de Comfaoriente EPS-S no cuenta especialmente con la documentación de sus procesos, sin embargo a través del reconocimiento del negocio se pudieron establecer sus procesos, para mayor entendimiento de los procesos se toman los 3 procesos principales y de ellos se derivan los subprocesos, de esta forma facilitando la asignación de funciones.

Figura 9.Procesos Principales de la dependencia



Fuente: Autores del proyecto LKYY

4.1.6. Actores Para la Dependencia

En el siguiente apartado se analizan cada uno de los procesos y subprocesos de Comfaoriente EPS-S teniendo en cuenta quien supervisa, cumple, produce, apoya, ejecuta, requiere y regula.

Cuadro 2.Cuadro de Actores

PROCESOS DEPENDENCIA SISTEMAS COMFAORIENTE EPS-S							
PROCESOS PRINCIPALES	**DESARROLLO**		**COORDINACION Y DEPURACION**			**SOPORTE TECNICO**	
SUBPROCESOS	**DESARROLLO E IMPLEMENTACION DE APLICATIVOS O MODULOS**	**MEJORA DE APLICATIVOS SIS_AUDITOR**	**COORDINACION Y PLANEACION DE DEPENDENCIA**	**DEPURACION BASE DE DATOS**	**REPORTES Y CARGUES DE INFORMACION**	**MANTENIMIENTO CORRECTIVO Y PREVENTIVO DE HARDWARE**	**MANTENIMIENTO CORRECTIVO Y PREVENTIVO DE SOFTWARE**
SUPERVISA	JEFE DE SISTEMAS	JEFE DE SISTEMAS	GERENCIA	GERENCIA	ENTES DE VIGILANCIA Y CONTROL Y GERENCIA	JEFE DE SISTEMAS	JEFE DE SISTEMAS
CUMPLE	Mejorar Continuamente la eficacia de nuestros procesos para contribuir a la satisfacción de nuestros clientes.	Mantener un proceso de mejora de acuerdo a las capacidades y conocimientos informáticos del personal.	Mejorar Continuamente la eficacia de nuestros procesos para contribuir a la satisfacción de nuestros clientes.	Procurar el mejoramiento, resguardo y la actualización de la información de los usuarios	Realizar los reportes de información correspondientes al área de sistemas a los entes de control en cumplimiento	Mantener un proceso de Innovación Tecnológica de acuerdo a las necesidades de la empresa	Mantener un proceso de Innovación Tecnológica de acuerdo a las necesidades de la empresa
PRODUCE	Sistema de Información adaptado a las necesidades de la empresa	Sistema de Información adaptado a las necesidades de la empresa	Documentación y supervisión área de Sistemas	Base de datos y Aplicativo web Actualizado, Backups	Consolidados de cargues de información y prestación de servicios de	Equipos óptimo funcionamiento	software en correcto funcionamiento

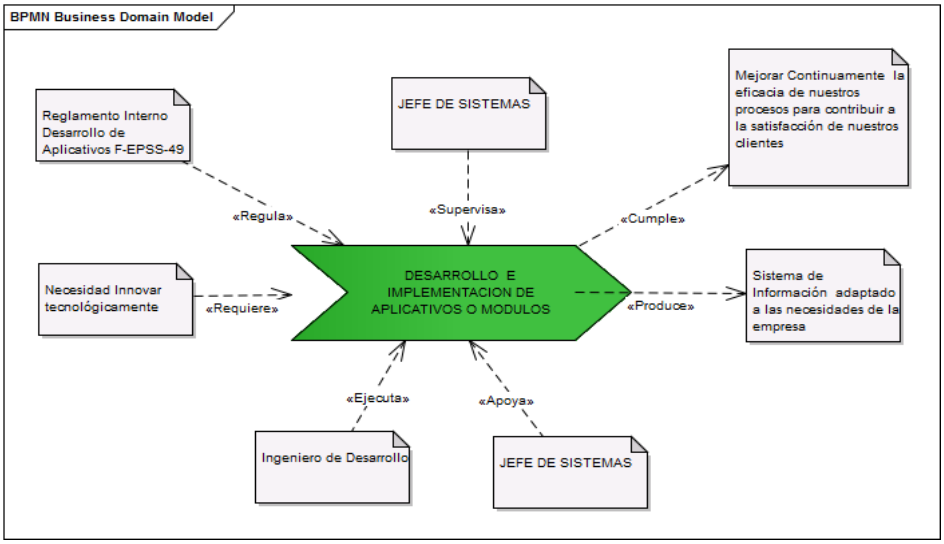
					afiliados		
APOYA	JEFE DE SISTEMAS	JEFE DE SISTEMAS	JEFE DE SISTEMAS	DESARROLLADOR Y TENICO	JEFES TODAS DEPENDENCIAS	JEFE DE SISTEMAS	JEFE DE SISTEMAS
EJECUTA	Ingeniero de Desarrollo	Ingeniero de Desarrollo	JEFE DE SISTEMAS	JEFE DE SISTEMAS	JEFE DE SISTEMAS	TECNICO	TECNICO
REQUIERE	Necesidad Innovar tecnológicamente	Necesidad Innovar tecnológicamente	Necesidad de Correcto funcionamiento dependencia de sistemas	Red prestadora y Entes vigilancia y control	Entes vigilancia y control Y MINSALUD	Usuarios de los Equipos para optimizar la automatización del trabajo.	Empleados Empresa y empresa para optimo desempeño laboral
REGULA	Reglamento Interno Desarrollo de Aplicativos F-EPSS-49	Reglamento Interno Desarrollo de Aplicativos F-EPSS-49	Reglamento Interno funciones Jefe de Sistemas	Reglamento Interno Bases de datos	Normatividad vigente MINSALUD	Reglamento Interno Soporte técnico	Reglamento Interno Soporte técnico

Fuente. Autores del proyecto LKYY

4.1.7. Diagramas De Los Subprocesos

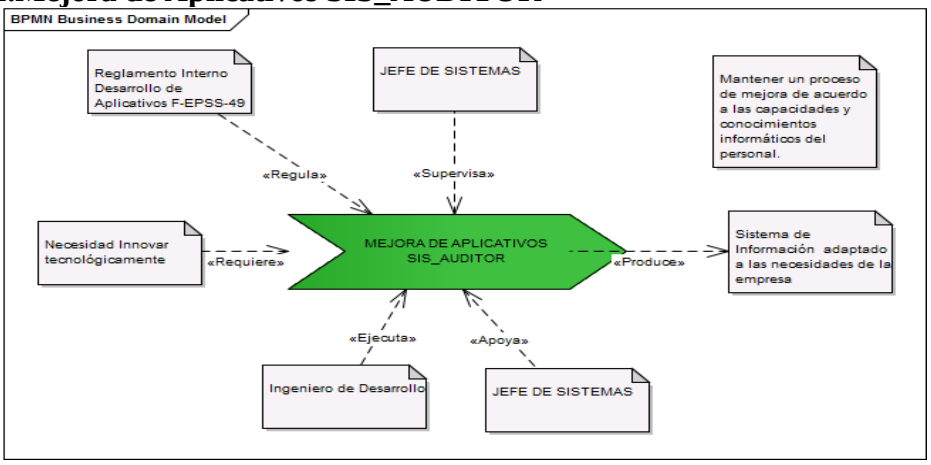
Una vez conocidos los actores involucrados en los procesos y subprocesos de Comfaoriente EPS-S se presentan cada uno de los diagramas.

Figura 10.Diagrama de Desarrollo e implementación de aplicativos o módulos



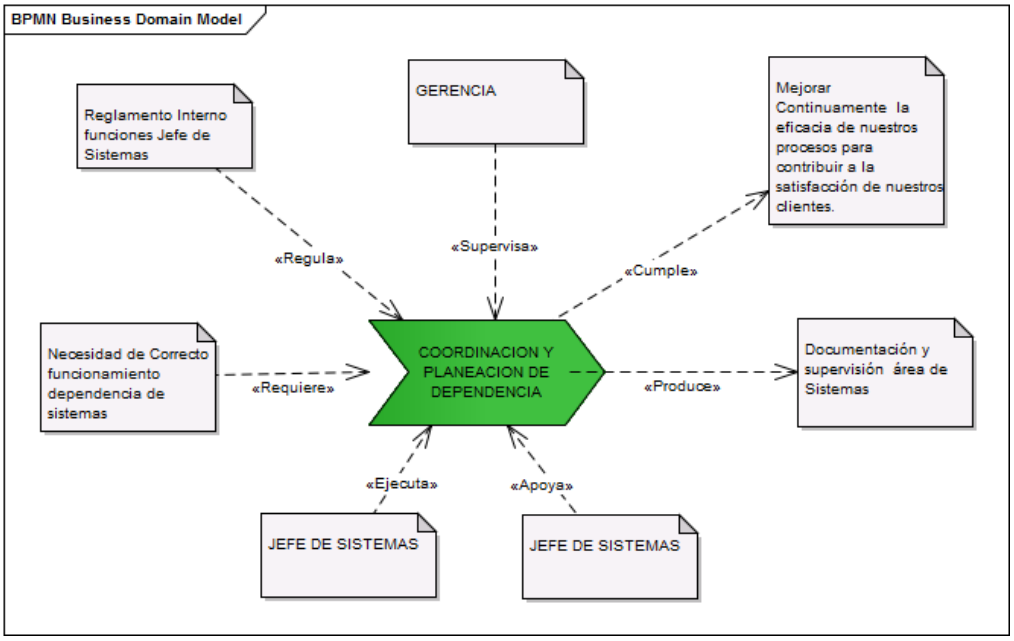
Fuente: Autores del proyecto LKYY

Figura 11.Mejora de Aplicativos SIS_AUDITOR



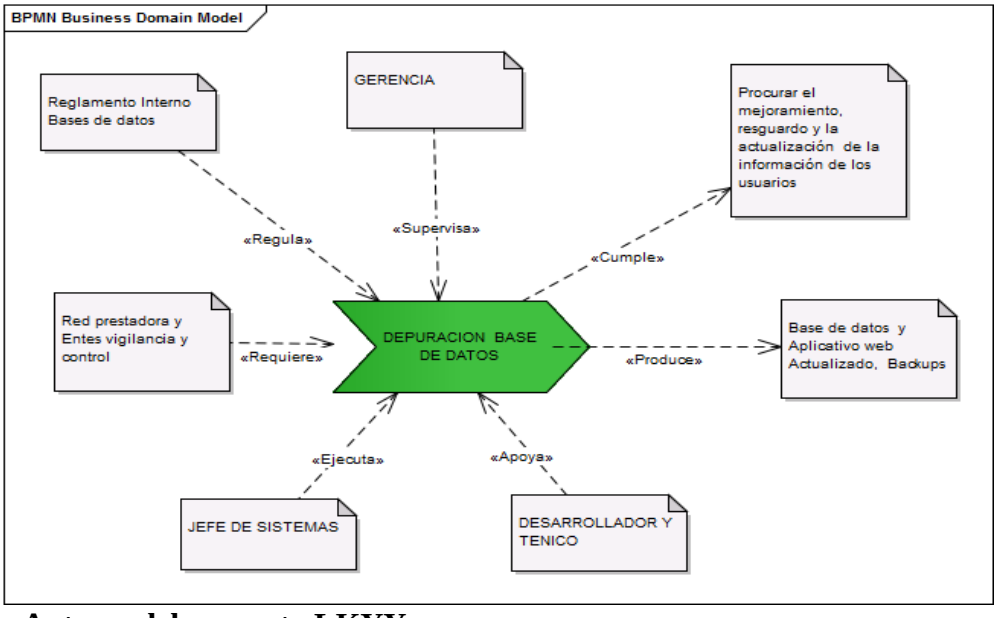
Fuente: Autores del proyecto LKYY

Figura 12.Coordinación y Planeación de Dependencia



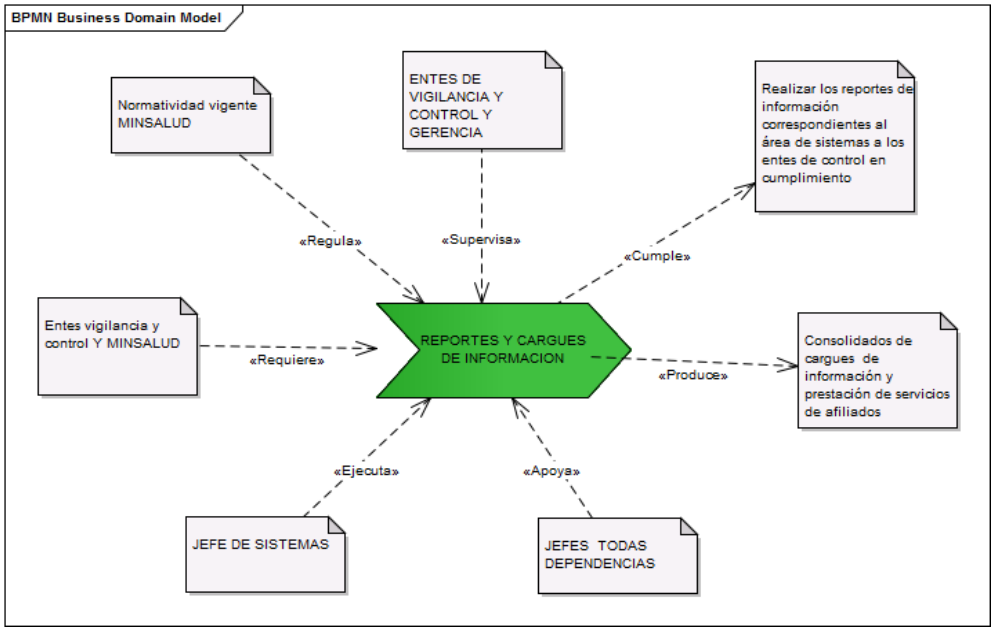
Fuente: Autores del proyecto LKYY

Figura 13.Depuración Base de Datos



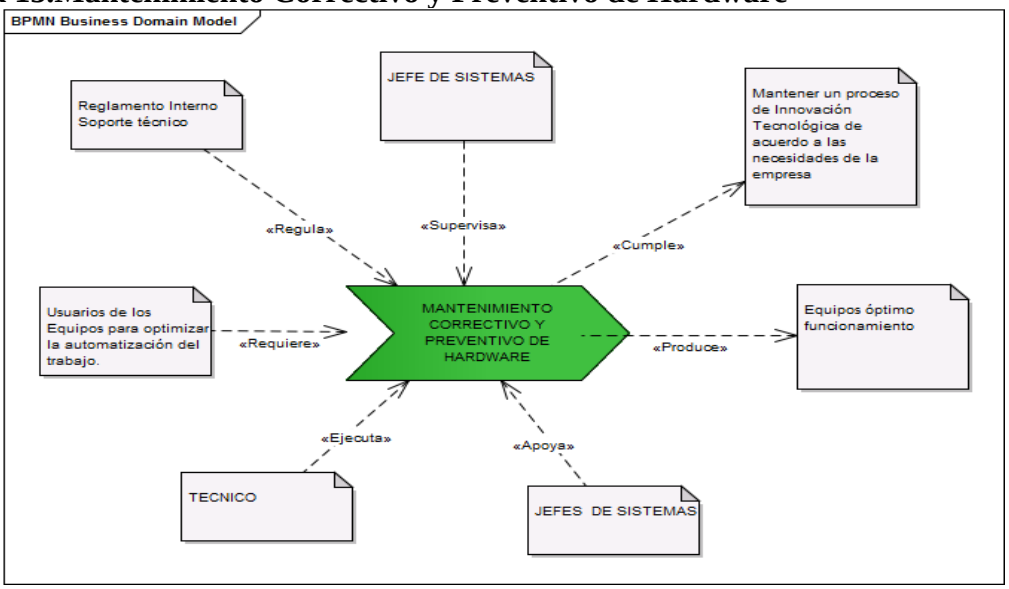
Fuente: Autores del proyecto LKYY

Figura 14.Reportes y Cargues de Información



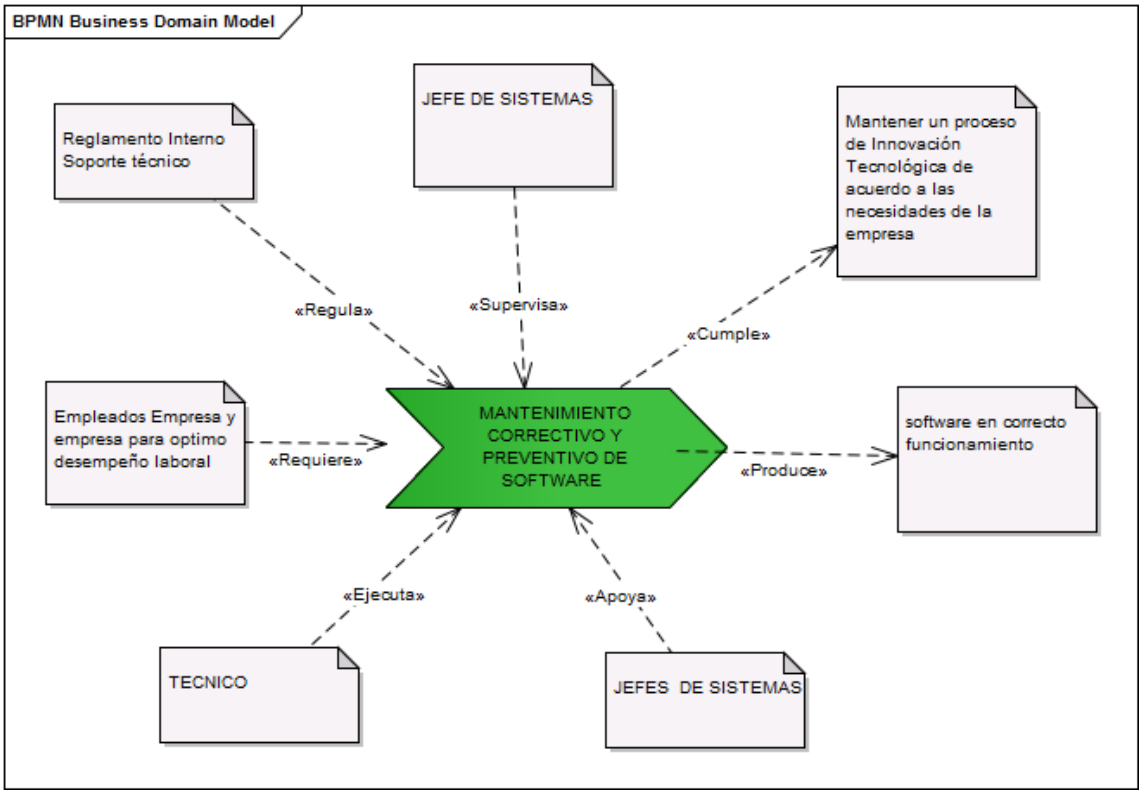
Fuente: Autores del proyecto LKYY

Figura 15.Mantenimiento Correctivo y Preventivo de Hardware



Fuente: Autores del proyecto LKYY

Figura 16.Mantenimiento Correctivo y Preventivo de Software

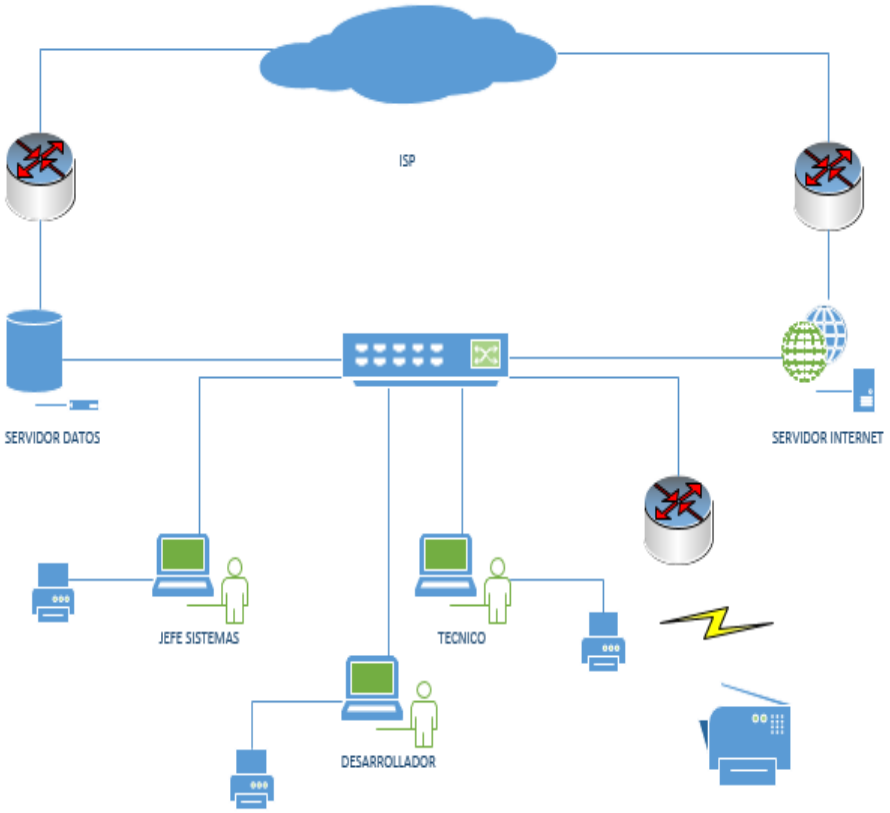


Fuente: Autores del proyecto LKYY

4.1.9 Propuesta Para la Infraestructura Tecnológica de la Dependencia Grupo Sistemas

Propuesta para la topología del grupo de área de sistemas. El tipo de red que utiliza es una LAN (Red de área Local) con topología tipo Estrella.

Figura 17.Topología de red



Fuente: Autores del Proyecto LKYY

4.1.10. Equipos

Cuadro 3. Características de equipos

Equipos	Características	Cantidad
Servidor web	Sistema operativo XP	1
Servidor para base de datos	Sistema Windows server 2003	1
Router cisco	permite el enrutamiento a cada uno de los equipos	2
Puntos de red		3
1 punto inalámbrico		1
Impresoras	*Hewlett-Packard*	3
Impresoras inalámbricas	*Hewlett-Packard*	1

Fuente: Autores del proyecto LKYY

4.1.11. Sistemas De Información

El Sistema de Información que utiliza la dependencia y todo el Programa del Régimen Subsidiado COMFAORIENTE es el Software SIS_AUDITOR que cuenta con las siguientes características en la dependencia:

SIS_AUDITOR - Está diseñado para ser operado por cualquier usuario con conocimientos básicos del ambiente Windows, unificado con los módulos que se manejan directamente desde el motor de Base de Datos FIREBIRD y un ODBC; los procedimientos y funciones se programan en lenguaje Visual Basic. Esta premisa incluye a cualquier persona inmersa en el mundo de la gestión y administración de planes y beneficios de salud; se ha diseñado para que guíe a personas con alguna experiencia mínima en el manejo de computadores, en la operación y funcionamiento del software **SIS_AUDITOR**.

Las ayudas gráficas y ejemplos del funcionamiento permiten al lector agilizar su comprensión sin incurrir en explicaciones arduas sobre el detalle técnico de los programas. Es intencionadamente breve, conciso y sencillo de seguir; en otras palabras, es para principiantes.

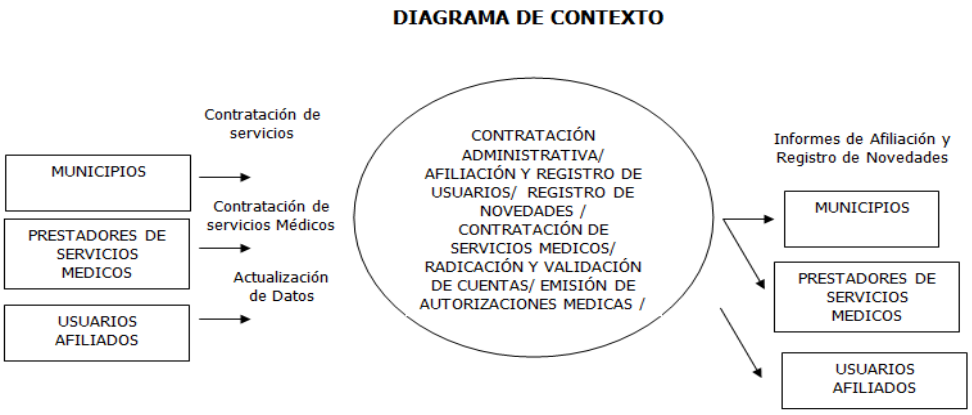
Teniendo en cuenta el crecimiento de la información, se pretende en un futuro la integración y migración a un motor de base más robusto como es el FIREBIRD, como ya se ha venido trabajando en algunos módulos.

4.3.2. Diseño lógico dependencia grupo sistemas

Este diagrama tiene como objetivo mostrar los eventos más generales que existen entre entidades o sistemas externos y el Sistema de Información del Programa EPS´S de la Caja de Compensación Familiar del Oriente Colombiano COMFAORIENTE

Figura 18.Diagrama de contexto

.

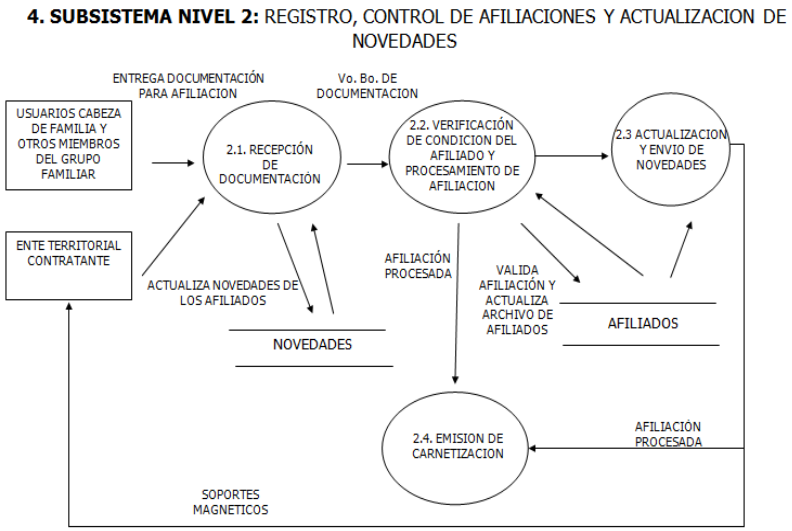


Fuente: documentos de la dependencia de sistemas de Comfaoriente EPS-S

Figura 19.Diagrama nivel 2 de afiliación y registró

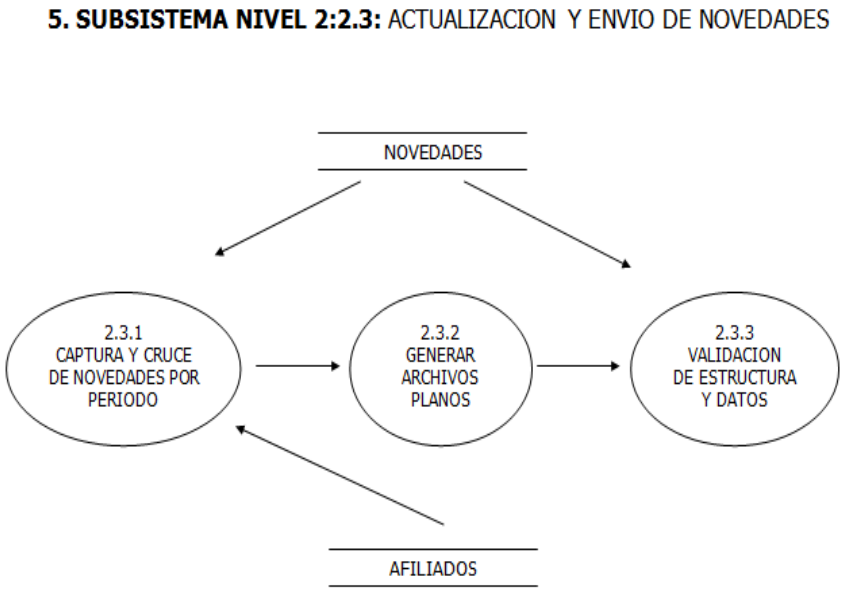
Fuente: Documentos de la dependencia de sistemas de Comfaoriente EPS-S

Figura 20.Diagrama subsistema nivel 2



Fuente: Documentos de la dependencia de sistemas de Comfaoriente EPS-S

Figura 21.Diagrama subsistema nivel 2:2:3



Fuente: Documentos de la dependencia de sistemas de Comfaoriente EPS-S

4.3.3. Sistema De Gestión De Base De Datos

La dependencia utiliza MySql para la aplicación Web, y para la administración de la base de datos general utiliza manager 2008 como base el motor Firebird.

4.1.10. Auditoria de Sistemas

Para el desarrollo de la auditoria se tuvieron en cuenta una serie de pasos para lograr caracterizar área y sus procesos y dimensionar el tamaño de la auditoria, el cual se explica en la siguiente figura.

Figura 22.Fases de Auditoria

Fuente: Autores del proyecto LKYY

Alcance y Objetivos de la Auditoria

Objetivo General

Lograr un manejo más eficiente y seguro de la información que servirá para un adecuado funcionamiento de la misma.

Objetivo Específicos

- Determinar la veracidad de la información que maneja la Dependencia del Grupo de Sistemas de Comfaoriente EPS-S.
- Evaluar los procesos con los que cuentan la dependencia del grupo de sistemas.
- Evaluar que se cumplan los procesos que maneja la dependencia del grupo de sistemas.
- Evaluar la forma como se administran los dispositivos de almacenamiento de la dependencia
- Evaluar el control que se tiene sobre el mantenimiento y las fallas de las Pcs.
- Comprobar la seguridad e integridad de la base de datos.
- Verificar los procedimientos de back-up.

Elaboración del plan y del programa de auditoria.

Retomando los resultados previos que se obtuvieron en el desarrollo del objetivo 1 se logró obtener información general sobre la empresa se tomó como investigación preliminar y de ella se planeó el programa de auditoria en el cual se discrimina el tiempo, costo, personal necesario y documentos auxiliares a solicitar y formular durante el desarrollo de la misma.

Administración

Se recopila la información para obtener una estructura general del departamento por medio de observaciones, entrevistas preliminares y los documentos solicitados para definir el objetivo y alcance de la auditoria.
La dependencia de sistemas de Comfaoriente EPS-S cuenta con diferentes tipos de recursos en su área, definidos tales como tecnológicos y de información, así como recurso humano que se encargan de la debida administración de los datos, entre estos se mencionan a continuación:

Recursos tecnológicos

- Rap
- Servidores
- Equipos de escritorio
- Portátiles
- Enrutadores
- Conmutadores de red
- Teléfonos
- Medios extraíbles (por ejemplo, cintas, disquetes, CD-ROM, DVD, discos duros portátiles, Dispositivos de almacenamiento PC Card, dispositivos de almacenamiento USB, etc.)
- Fuentes de alimentación
- Sistemas contra incendios
- Sistemas de aire acondicionado

Software Y Datos

- Manual de Proceso y procedimientos
- Manual del Sistema de Información SIS_AUDITOR
- Bases de datos de facturas
- Bases de datos de Autorizaciones
- Bases de datos contratos Red de servicios
- Base de datos Referencias
- Backups
- Correo Electrónico

- Página Web
- Base de datos de Contraseñas
- Chat Interno BIG ANT
- Llamadas Telefónicas
- Software de aplicación de servidor
- Software de aplicación de usuario final
- Herramientas de desarrollo
- Sistema de Información SIS_AUDITOR
- Antivirus

Recursos humanos

- Ingeniero de Desarrollo
- Jefe de Sistemas
- Personal Técnico Informático
- Limpieza de Dependencia
- Servicio de Mensajería

Personal participante

A continuación se presenta un cuadro con el personal participante de la Auditoria

Cuadro 4. Personal participante

Equipo auditor	Profesión o Cargo	Perfil
Leidy Lisbeth Contreras Hernández	Ingeniera en telecomunicaciones	Profesional capaz de enfrentar, investigar, diseñar, simular, construir, implementar, apropiar y aplicar las Tecnologías de la información y las comunicaciones, en el procesamiento, transmisión y almacenamiento de la información; que además le permite formular, planificar, evaluar, asesorar, y liderar proyectos de Telecomunicaciones acordes con la legislación y la normatividad.
Vianny Karina Buitrago Sepúlveda	Ingeniera de Sistemas	Profesional capaz de modelar estructuras y procesos organizativos, diseñar y administrar los recursos de tecnología de información, construir e implantar aplicaciones de tecnología informática, así como de diseñar soluciones a problemas complejos.
Yeinny Yohana Acosta Vergel	Contador Público	Profesional capaz de desempeñarse como contadores de empresas privadas y

		públicas, auditores, revisores fiscales, asesores tributarios, analistas financieros, contralores, asesores independientes, analistas o jefes contables, perito evaluador, director de presupuesto y jefe de control interno.
Yorman José Márquez Fuentes	Contador Público	Profesional capaz de desempeñarse como contadores de empresas privadas y públicas, auditores, revisores fiscales, asesores tributarios, analistas financieros, contralores, asesores independientes, analistas o jefes contables, perito evaluador, director de presupuesto y jefe de control interno.

Fuente: Autores del proyecto LKYY

4.1.11. ESTUDIO DEL NEGOCIO

En la etapa de reconocimiento realizado a la Dependencia del área de sistemas de Comfaoriente EPS-S, se aplicaron instrumentos de recolección de información, los cuales arrojaron datos valiosos, que brindan soporte fundamental para el desarrollo del objetivo de la presente propuesta.

La información suministrada por la dependencia del área de sistemas, está expuesta permanentemente a riesgos que comprometen su disponibilidad, integridad y confidencialidad. Con el fin de apoyar la seguridad de dicha información se propone diseñar una política de Gestión de seguridad de la información, por tanto se aplican los siguientes cuestionarios a cuatro funcionarios de la dependencia con base en la norma 27001:2013 .

Tabulación de Instrumentos Aplicados

En la etapa de reconocimiento realizado a la Dependencia del área de sistemas de Comfaoriente EPS-S, se aplicaron instrumentos de recolección de información, los cuales arrojaron datos valiosos, que brindan soporte fundamental para el desarrollo del objetivo del presente proyecto.

La información de la dependencia de sistemas de Comfaoriente EPS-S está expuesta permanentemente a riesgos que comprometen su disponibilidad, integridad y confidencialidad y con el fin de apoyar la seguridad de dicha información se propone diseñar una política de Gestión de seguridad de la información, por tanto se aplican los siguientes cuestionarios a tres funcionarios de la dependencia con base en la norma 27001:2013 para realizar un diagnóstico de la misma.

	TABULACIÓN DE CUESTIONARIOS APLICADOS	
	Dependencia de Sistemas de COMFAORIENTE EPS-S	Proceso: Norma ISO 27001 : 2013
	Entrevistado Nº 1	

A.5 Políticas de seguridad de la información

Evaluación de medidas, controles, procedimientos, normas y estándares de seguridad así como contraseñas y autorización del personal de Comfaoriente EPS-S.

	POLITICAS DE SEGURIDAD DE LA INFORMACION			
	PREGUNTAS	**RESPUESTAS**		
		SI	**NO**	**N/A**
	12	7	4	1

Fuente: Autores del Proyecto LKYY

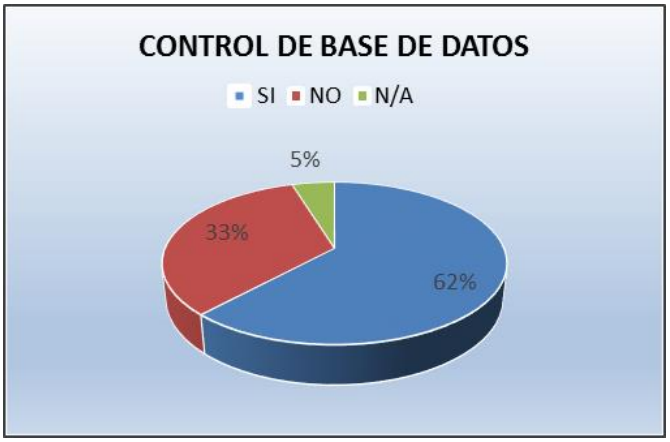
Fuente: Autores del Proyecto LKYY

A.6 Control de base de datos

Evaluación de Seguridad de la información de la base de datos de Comfaoriente EPS-S.

	CONTROL DE BASE DE DATOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	21	13	7	1

Fuente: Autores del Proyecto LKYY



Fuente: Autores del Proyecto LKYY

A.13 Redes y comunicaciones

Evaluación de la infraestructura de redes de comunicación, instalación y diseños de redes de Comfaoriente EPS-S.

	REDES Y COMUNICACIONES			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	21	14	7	0

Fuente: Autores del Proyecto LKYY

Fuente: Autores del Proyecto LKYY

A.11 Seguridad fisica y del entorno

Evaluación de toda la seguridad fisica de Comfaoriente EPS-S.

	SEGURIDAD FISICA Y DEL ENTORNO			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	5	2	3	0

Fuente: Autores del Proyecto LKYY

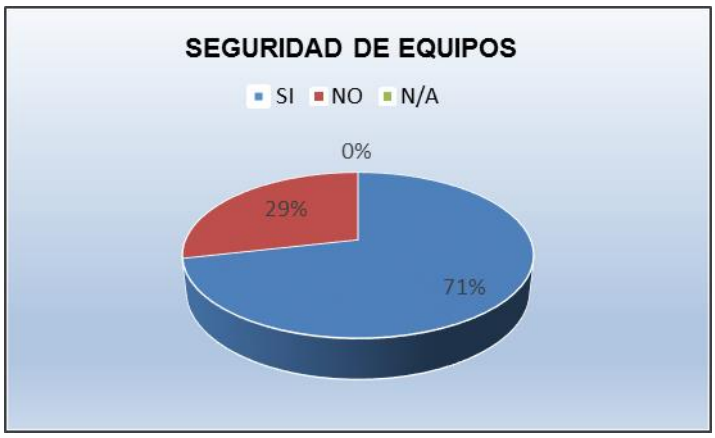
Fuente: Autores del Proyecto LKYY

A.11. 2 Seguridad de equipos

Evaluación de todos los equipos que hacen parte de la dependencia de sistemas de Comfaoriente EPS-S

	SEGURIDAD DE EQUIPOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	7	5	2	0

Fuente: Autores del Proyecto LKYY



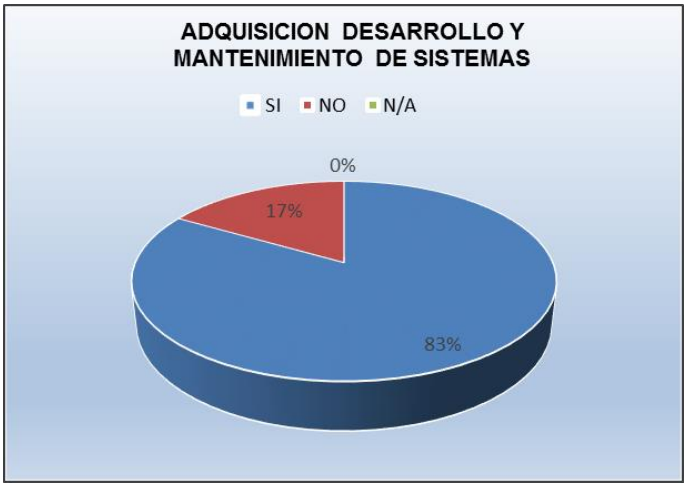
Fuente: Autores del Proyecto LKYY

A.14 Adquisición, desarrollo y mantenimiento de sistemas

Evaluar la seguridad de la información con respecto a los procesos de desarrollo de soporte de Comfaoriente EPS-S.

	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	6	5	1	0

Fuente: Autores del Proyecto LKYY



Fuente: Autores del Proyecto LKYY

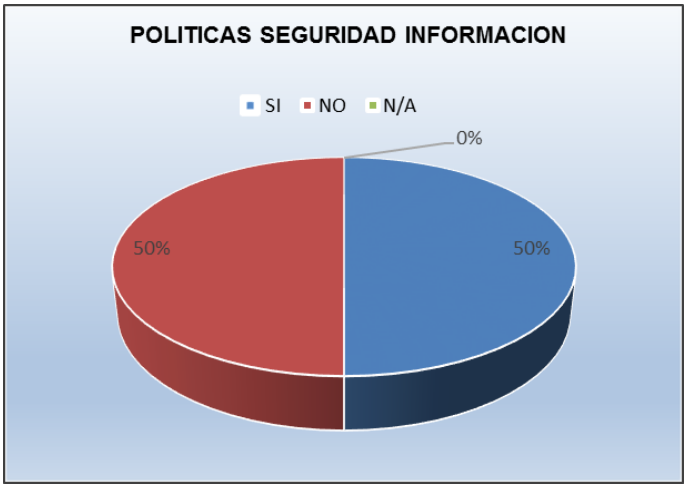
	TABULACIÓN DE CUESTIONARIOS APLICADOS	
	Dependencia de Sistemas de COMFAORIENTE EPS-S	Proceso: Norma ISO 27001 : 2013
	Entrevistado Nº 2	

A.5 Políticas de seguridad de la información

Evaluación de medidas, controles, procedimientos, normas y estándares de seguridad así como contraseñas y autorización del personal de Comfaoriente EPS-S.

	POLITICAS DE SEGURIDAD DE INFORMACIÓN			
	PREGUNTAS	**RESPUESTAS**		
		SI	**NO**	**N/A**
	12	6	6	0

Fuente: Autores del Proyecto LKYY



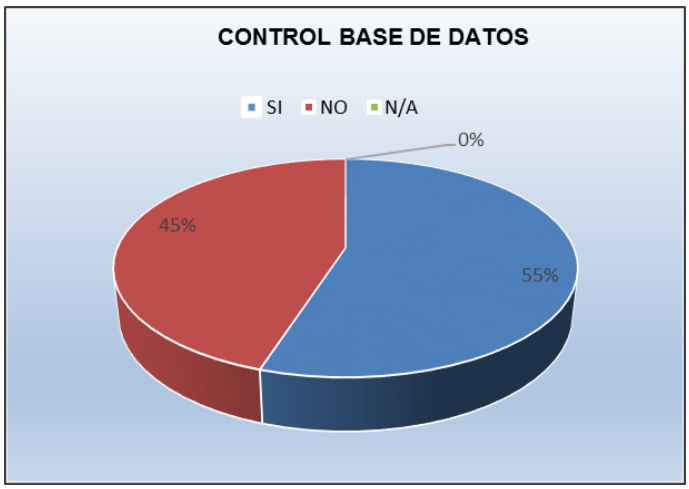
Fuente: Autores del Proyecto LKYY

A.6 Control de base de datos

Evaluación de Seguridad de la información de la base de datos de Comfaoriente EPS-S.

	CONTROL DE BASE DE DATOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	20	11	9	0

Fuente: Autores del Proyecto LKYY



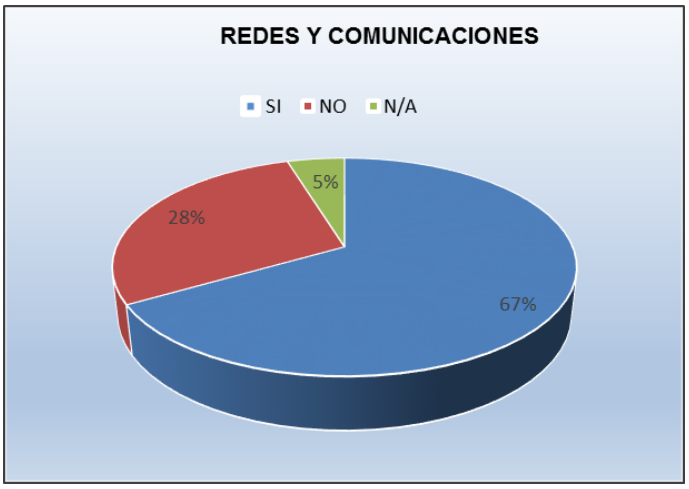
Fuente: Autores del Proyecto LKYY

A.13 Redes y comunicaciones

Evaluación de la infraestructura de redes de comunicación, instalación y diseños de redes de Comfaoriente EPS-S.

	REDES Y COMUNICACIONES			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	21	14	6	1

Fuente: Autores del Proyecto LKYY



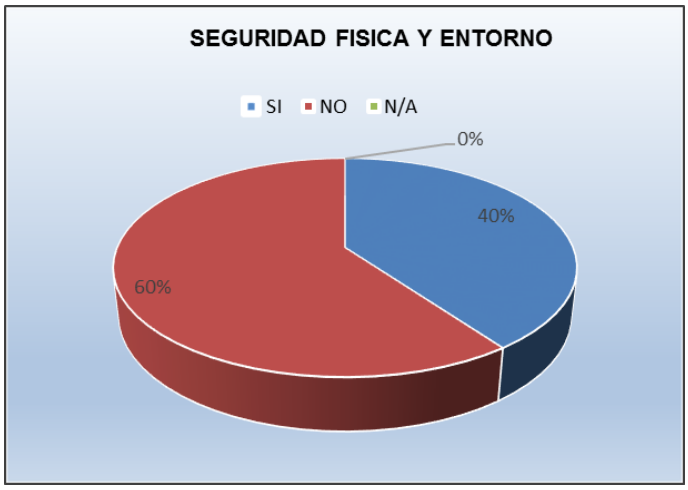
Fuente: Autores del Proyecto LKYY

A.11 Seguridad fisica y del entorno

Evaluaciòn de toda la seguridad fisica de Comfaoriente EPS-S.

	SEGURIDAD FISICA Y DEL ENTERNO			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	5	2	3	0

Fuente: Autores del Proyecto LKYY



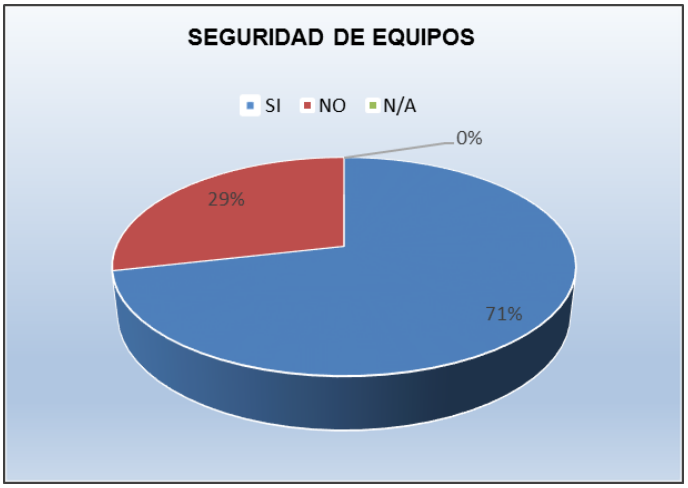
Fuente: Autores del Proyecto LKYY

A.11.2 Seguridad de equipos

Evaluación de todos los equipos que hacen parte de la dependencia de sistemas de Comfaoriente Eps-s.

	SEGURIDAD DE EQUIPOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	7	5	2	0

Fuente: Autores del Proyecto LKYY



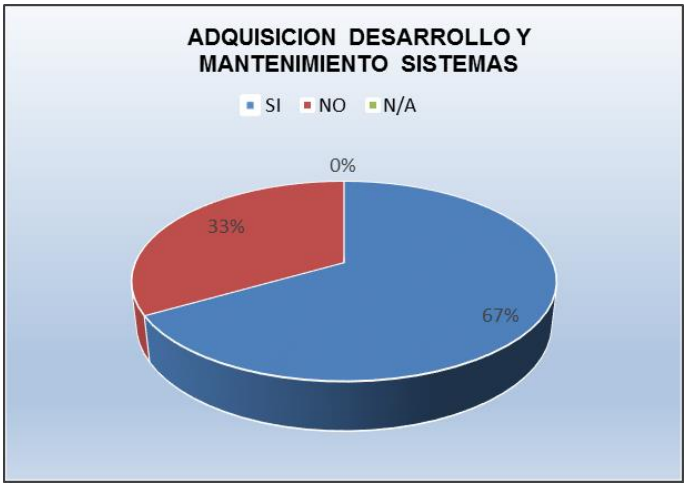
Fuente: Autores del Proyecto LKYY

A.14 Adquisición, desarrollo y mantenimiento de sistemas

Evaluar la seguridad de la información con respecto a los procesos de desarrollo de soporte de Comfaoriente EPS-S.

	ADQUISICIÓN, DESARROLLOY MANTENIMIENTO DE SISTEMAS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	6	4	2	0

Fuente: Autores del Proyecto LKYY



Fuente: Autores del Proyecto LKYY

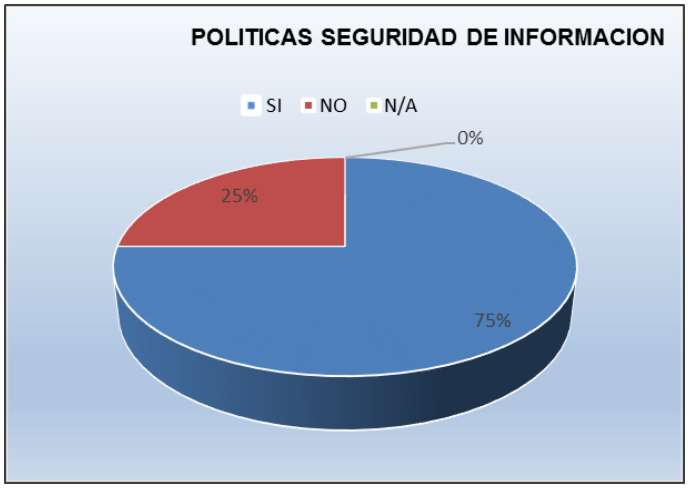
	TABULACIÓN DE CUESTIONARIOS APLICADOS	
	Dependencia de Sistemas de COMFAORIENTE EPS-S	Proceso: Norma ISO 27001 : 2013
	Entrevistado Nº 3	

A.5 Políticas de seguridad de la información

Evaluación de medidas, controles, procedimientos, normas y estándares de seguridad así como contraseñas y autorización del personal de Comfaoriente EPS-S.

	POLITICAS DE SEGURIDAD DE INFORMACIÓN			
	PREGUNTAS	**RESPUESTAS**		
		SI	**NO**	**N/A**
	12	9	3	0

Fuente: Autores del Proyecto LKYY



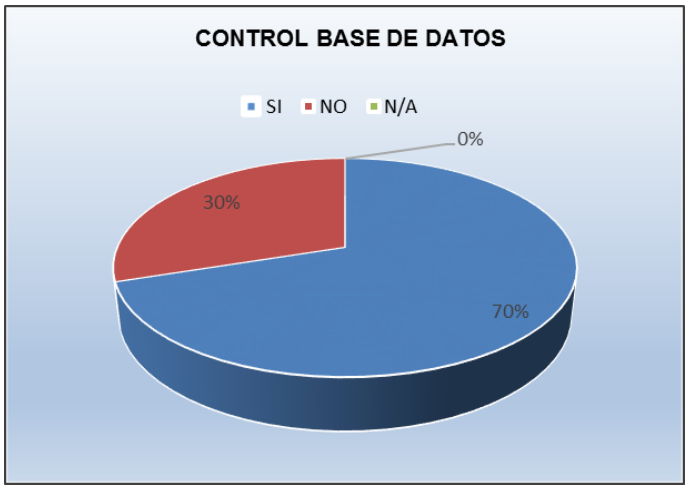
Fuente: Autores del Proyecto LKYY

A.6 Control de base de datos

Evaluación de Seguridad de la información de la base de datos de Comfaoriente EPS-S

	CONTROL DE BASE DE DATOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	20	14	6	0

Fuente: Autores del Proyecto LKYY



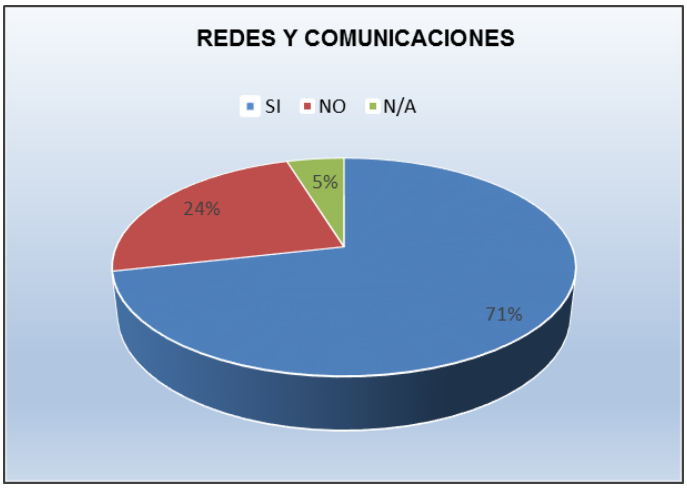
Fuente: Autores del Proyecto LKYY

A.13 Redes y comunicaciones

Evaluación de la infraestructura de redes de comunicación, instalación y diseños de redes de Comfaoriente EPS-S.

	REDES Y COMUNICACIONES			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	21	15	5	1

Fuente: Autores del Proyecto LKYY



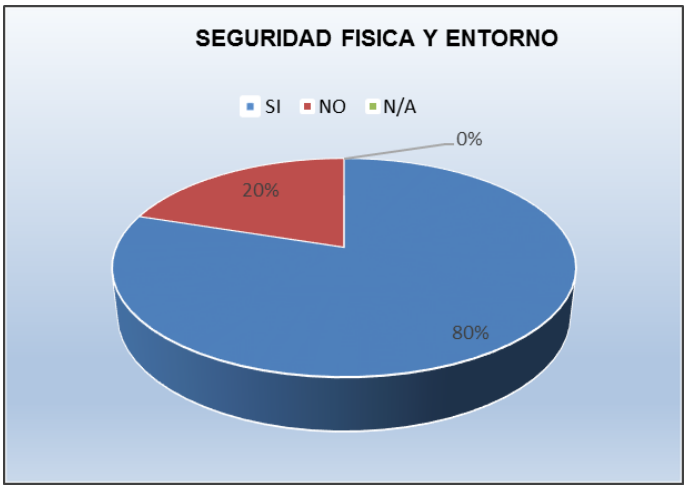
Fuente: Autores del Proyecto LKYY

A.11 Seguridad fisica y del entorno

Evaluaciòn de toda la seguridad fisica de Comfaoriente EPS-S.

	SEGURIDAD FISICA Y DEL ENTORNO			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	5	4	1	0

Fuente: Autores del Proyecto LKYY



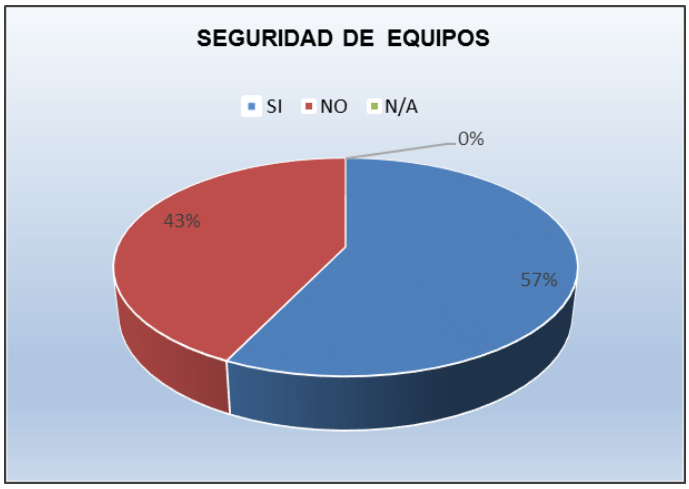
Fuente: Autores del Proyecto LKYY

A.11.2 Seguridad de equipos

Evaluación de todos los equipos que hacen parte de la dependencia de sistemas de Comfaoriente EPS-S.

	SEGURIDAD DE EQUIPOS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	7	4	3	0

Fuente: Autores del Proyecto LKYY



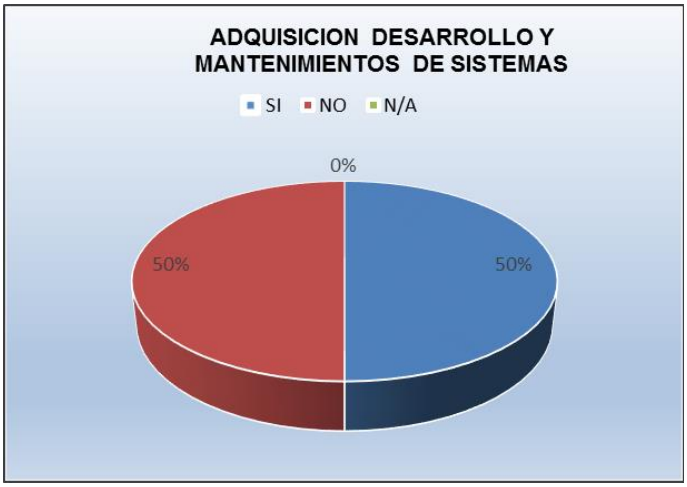
Fuente: Autores del Proyecto LKYY

A.14 Adquisición, desarrollo y mantenimiento de sistemas

Evaluar la seguridad de la información con respecto a los procesos de desarrollo de soporte de Comfaoriente EPS-S.

	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
	PREGUNTAS	RESPUESTAS		
		SI	NO	N/A
	6	3	3	0

Fuente: Autores del Proyecto LKYY



Fuente: Autores del Proyecto LKYY

Una vez realizada la auditoria pasiva, con base en el estudio de negocio y la aplicación de instrumentos a tres funcionarios de la dependencia de sistemas de Comfaoriente Eps-s evaluando algunos dominios de la norma 27001:2013 tales como: Políticas de Seguridad de la información, Organización de la seguridad de la Información, Seguridad de las Comunicaciones, Seguridad física y del Entorno, Seguridad de Equipos, adquisición, desarrollo y mantenimiento de Equipos, se establecerán como base para el desarrollo de la política de seguridad.

4.1.12. Informe de auditoria

Una vez realizada la auditoria pasiva a la dependencia de Sistemas de COMFAORIENTE EPS-S evaluando algunos aspectos siguiendo la norma 27001:2013 tales como: Red, Seguridad física, Seguridad lógica, Controles de accesos al software que maneja la

dependencia, Controles del sitio web que maneja la dependencia, Planes de contingencia y procedimientos de respaldo de la información se evidenció que:

- Del análisis del negocio que se hizo previamente se observó que la dependencia no cuenta con una estructura como la de organigrama por tanto se recomienda realizar su diseño. (Los autores de proyecto plantean el diseño el cual esta anexo.)

Del mismo modo se recomienda:

- Adquisición de un nuevo antivirus para los equipos de la dependencia.
- Creación de los inventarios de hardware y de software así como la ejecución de actualizaciones programadas.
- Actualización de los controles de cambios del sistema de Información.
- Diseño del proceso de segmentación de la red, incluyendo cambios que se puedan presentar en la topología.
- Actualización del plan de contingencia para evitar futuros inconvenientes en caso de presentarse alguna emergencia y puedan ocasionar problemas legales.
- Implementar un sistema para el registro de las personas que ingresan a la dependencia.

4.2. Identificar los riesgos que exponen la seguridad de la información de la dependencia de sistemas de Comfaoriente EPS-S.

En la siguiente sección identificaremos los riesgos presentes en la dependencia de sistemas de Comfaoriente EPS-S con base en los tres elementos más importantes: Activos, Amenazas y Vulnerabilidades, teniendo en cuenta la metodología PHVA y en conformidad con la norma ISO/IEC 27001/2013

4.2.1 Propiedad De Activos

Para analizar la propiedad de los activos de Comfaoriente EPS-S se verificaron que los entes que interactúan en ellos son los siguientes. Tomando como base MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA, entregable 3, 4, 5, 6 informe final[6].

Cuadro 5. Entes que actúan en los activos

TIPO ACTIVO	ACTIVO	PROPIEDAD		
		PROPIETARI	CUSTODIO	USUARIO

[6] MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA, entregable 3, 4, 5, 6 informe final

		O		
SISTEMAS E INFRAESTRUTURA	Rap	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Router	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	switch	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Firewall	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Servidores	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Equipos de Escritorio	Dependencia de Sistemas	Profesionales Administrativos	Profesionales Administrativos
	Portátiles	Dependencia de Sistemas	Profesionales Administrativos	Profesionales Administrativos
	Impresoras	Dependencia de Sistemas	Profesionales Administrativos	Profesionales Administrativos
	Discos duros externos	Dependencia de Sistemas	Jefe de Sistemas	Técnico
	Aire Acondicionado	Dependencia de Sistemas	Técnico	Profesionales Administrativos
	Teléfonos	Dependencia de Sistemas	Profesionales Administrativos	Profesionales Administrativos
	Fuentes de Alimentación	Dependencia de Sistemas	Técnico	Técnico
	Sistema Contra Incendio	Dependencia de Sistemas	Técnico	Técnico
	USB	Dependencia de Sistemas	Profesionales Administrativos	Profesionales Administrativos
SOFTWARE Y DATOS	Manual de Procesos y Procedimientos dependencia de Sistemas	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Manual	Dependencia de	Jefe de	Jefe de

	Sistema de Información	Sistemas	Sistemas	Sistemas
	Base de datos Facturas	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Base de datos Autorizaciones	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Base de datos de Contratos Red de Servicios	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Base de Datos Básicos Usuarios	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Base de datos Números Telefónicos referencia	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Backups	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Correo Electrónico	Dependencia de Sistemas	Jefe de Sistemas	Profesionales Administrativos
	Página web	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Base de datos de Contraseñas	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Chat Interno BIG ANT	Dependencia de Sistemas	Jefe de Sistemas	profesionales Administrativos
	Llamadas telefónicas	Dependencia de Sistemas	Jefe de Sistemas	Profesionales Administrativos
	Software de aplicación del servidor	Dependencia de Sistemas	Técnico	profesionales Administrativos
	Software de Aplicación de Usuario final	Dependencia de Sistemas	Técnico	Profesionales Administrativos
	herramientas de desarrollo	Dependencia de Sistemas	Ingeniero de Desarrollo	Ingeniero de Desarrollo

	Sistema de Información SIS-Auditor	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
	Antivirus	Dependencia de Sistemas	Técnico	Profesionales Administrativos
	Base de datos de RIPS	Dependencia de Sistemas	Ingeniero de Desarrollo	Profesionales Administrativos
PERSONAL	Personal Técnico Informático	Dependencia de Sistemas	Asistente Técnico	Asistente Técnico
	Ingeniero de Desarrollo	Dependencia de Sistemas	Ingeniero de Desarrollo	Ingeniero de Desarrollo
	Jefe de Sistemas	Dependencia de Sistemas	Jefe de Sistemas	Jefe de Sistemas
	Limpieza de Dependencia	Talento Humano	Asistente Servicios Generales	Asistente Servicios Generales
	Servicio de Mensajería	Talento Humano	Asistente de mensajería	Asistente de mensajería

Fuente: Autores del proyecto LKYY

4.2.2 Impacto

Una vez identificados los activos de información que posee la empresa COMFAORIENTE EPS-S para cada uno de los procesos que se han decidido incluir dentro del alcance del SGSI, se identifica cual sería el impacto que tendría en su respectivo proceso la pérdida o alteración de cada uno de los activos identificados.

Entiéndase impacto como el grado en el que se ve afectado determinado sistema, en este caso proceso, al alterar uno de sus componentes, para este caso activos de información. A mayor correlación entre el resultado del proceso y la alteración del activo, el impacto de ese activo será mayor.

Generalmente la evaluación del impacto viene de criterios subjetivos de los conocedores del proceso, en este documento se utilizan tres requisitos propios de los activos de información de una empresa, como lo describe la Norma técnica Colombiana NTC-ISO/IEC 27001:2013[7] (Confidencialidad, Integridad y Disponibilidad), mediante los cuales se busca cuantificar el impacto que tiene dentro de su proceso.

[7] Norma técnica Colombiana NTC-ISO/IEC 27001:2013

Para cada requisito se establecieron tres niveles de impacto (bajo, mediano y alto) según se comporte el activo dentro de la dependencia, al momento de decidir cuál de los tres niveles aplica para cada categoría se realizó una cuantificación final de un acuerdo general del grupo, el ejercicio se realizó tomando activo por activo, evaluando los tres requisitos antes de continuar con el siguiente.

Tabla 1. Impacto

REQUISITOS CONFIDENCIALIDAD (C)		
VALOR DEL ACTIVO	**CLASE**	**DESCRIPCION**
BAJO	Disponible al publico	La información no sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles para el público.
MEDIANO	Para uso interno exclusivamente o uso restringido solamente	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles dentro de la organización con restricciones variadas con base en las necesidades de la empresa.
ALTO	Confidencial o Estrictamente confidencial	La información sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles sólo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procesamiento de información y los recursos del sistema están disponibles sólo sobre la base de la necesidad estricta del conocimiento.
REQUISITOS INTEGRIDAD (I)		
VALOR DEL ACTIVO	**CLASE**	**DESCRIPCION**
BAJO	Baja Integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el impacto en la empresa es insignificante o menor.
MEDIANO	Integridad Mediana	El daño o modificación no autorizada no es crítico

		Pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.
ALTO	Integridad Alta o Muy Alta	El daño o modificación no autorizada es crítica para las aplicaciones empresariales y el impacto en la empresa es importante y podría conllevar a la falta grave o total de la aplicación empresarial.
REQUISITOS DISPONIBILIDAD (D)		
VALOR DEL ACTIVO	**CLASE**	**DESCRIPCION**
BAJO	Baja Disponibilidad	Se puedes tolerar que el activo no esté disponible por más de un día.
MEDIANO	Disponibilidad Mediana	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día.
ALTO	Alta Disponibilidad	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas, o incluso menos

Fuente: http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

IMPACTO DE LOS ACTIVOS DE COMFAORIENTE EPS-S

Tabla 2. Impacto de los activos de Comfaoriente

TIPO ACTIVO	NOMBRE	C	D	I	VALOR ACTIVO
SISTEMAS E INFRAESTRUTURA	Rap	A	A	M	A
	Router	A	A	M	A
	swith	A	A	M	A
	Firewall	A	A	M	A
	Servidores	A	A	A	A
	Equipos de Escritorio	M	M	B	M
	Portatiles	M	M	B	M
	Impresoras	M	M	B	M
	Discos duros externos	M	B	B	M
	Aire Acondicionado	B	A	B	M
	Telefonos	B	A	M	M
	Fuentes de Alimentacion	M	A	M	A
	Sistema Contra Incendio	A	B	A	A
	USB	M	B	B	M
SOFTWARE Y DATOS	Manual de Procesos y Procedimientos dependencia de Sistemas	M	B	M	M
	Manual Sistema de Informacion	M	B	M	M
	Base de datos Facturas	A	A	A	A
	Base de datos Autorizaciones	A	A	A	A
	Base de datos de Contratos Red de Servicios	A	B	A	A
	Base de Datos Basicos Usuarios	A	A	A	A
	Base de datos Numeros Telefonicos referencia	A	A	M	A
	Backups	A	A	A	A
	Correo Electronico	M	A	A	A
	Pagina web	B	A	M	M
	Base de datos de Contraseñas	A	A	M	A
	Chat Interno BIG ANT	B	B	M	M
	Llamadas telefonicas	B	M	M	M
	Sotfware de aplicación del servidor	B	A	M	M
	Software de Aplicación de Usuario final	B	A	M	M
	herramientas de desarrollo	M	A	M	A
	Sistema de Informacion SIS-Auditor	B	A	M	M
	Antivirus	B	A	A	A
	Base de datos de RIPS	A	B	A	A
PERSONAL	Personal Tecnico Informático	B	B	M	M
	Ingeniero de Desarrollo	B	A	A	A
	Jefe de Sistemas	B	A	A	A
	Limpieza de Dependencia	B	B	B	B
	Servicio de Mensajería	B	B	B	B

C: Confidencialidad I: Integridad D: Disponibilidad

Fuente: Autores del proyecto LKYY

Por tanto de acuerdo a la valoración de los activos con base en términos de la confidencialidad, integridad y disponibilidad se observa su valoración cualitativa en la tabla 2 de acuerdo a los parámetros descritos en la tabla 3.

Tabla 3. Valoración cualitativa

VALOR DEL ACTIVO	DESCRIPCION
BAJO	La pérdida de confidencialidad, integridad o disponibilidad del activo no tiene ningún impacto en la Empresa
MEDIANO	La pérdida de confidencialidad, integridad o disponibilidad del activo impacta de manera importante la Empresa
ALTO	La pérdida de confidencialidad, integridad o disponibilidad del activo impacta negativamente la Empresa

Fuente: Autores del proyecto LKYY

4.2.3 Identificación De Amenazas

Las amenazas son entes o escenarios de tipo interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la organización, por tanto según encuesta y pruebas realizadas en Comfaoriente Eps-s se identificaron las siguientes amenazas clasificadas según el tipo y su origen.

Tabla 4. Clasificación de amenazas

ORIGEN	NOMENCLATURA
Agentes Naturales	N
Agentes Externos	E
Agentes Internos	I
Intencionalidad	D

Fuente: Autores del proyecto LKYY

Tabla 5. Identificación de Amenazas

TIPO	AMENAZA	ORIGEN
LEGALIDAD Y CRIMINALIDAD	Virus	I,D
	Infiltración	E,I
	Intrusión a red interna	E,D
	Hurto de Información	E,D
	Hurto físico	E,D
	Fraude	E,D
	Daños por vandalismo	E,D
FISICO	Incendio	E,I,D
	Inundación	N
	Sismo	N
	Falla eléctrica	E
NEGLIGENCIA PERSONAL	Mal manejo de sistemas y Herramientas informáticas	I
	Utilización de programas no autorizados	I
	Perdida de datos	E,I,D
	Infección de sistema por uso de portables sin escaneo	I,D
	Manejo inadecuado de contraseñas	I
	Fallas de Acceso a Archivos	I
	Acceso Electrónico no autorizado	I
	Red cableada expuesta a exceso no autorizado	I
	Daño Físico Irreparable	i

Fuente: Autores del proyecto LKYY

4.2.4 Identificación De Vulnerabilidades

Las vulnerabilidades[8] son elementos que pueden ser aprovechados por un atacante para violar la seguridad causando daños por si mismos sin tratarse de un ataque intencionado.

[8] BURGOS, Jorge y CAMPOS, Pedro. Modelo Para Seguridad de la Información en TIC. 2008, versión 2. Available from Internet: <ceur-ws.org/Vol-488/paper13.pdf>

Las vulnerabilidades son consideradas elementos internos de las empresas por lo tanto es tarea del jefe de sistema o administradores de red y usuarios detectarlos, valorarlos y reducirlos.

Una vez realizado el análisis de las amenazas que posee la dependencia de sistemas de Comfaoriente Eps-s se encuentra que son originadas por las siguientes vulnerabilidades las cuales se clasificaron según la parte física, natural, software, red y factor humano.

Tabla 6. Identificación de vulnerabilidades

TIPO	VULNERABILIDAD	AMENAZAS
FISICO	Ingreso de personal no autorizado a la dependencia de sistemas	Hurto de Información, Hurto físico
	La ubicación de la dependencia de sistemas está ubicada en el primer piso al lado de un baño.	Inundación
	No existe mantenimiento del cableado eléctrico interno y externo	Falla eléctrica
NATURAL	La estructura del edificio de Comfaoriente Eps-s es muy antiguo y no posee una construcción segura anti sismos	sismo
SOFTWARE Y HARDWARE	El Servidor no cuenta con la capacidad necesaria para soportar el flujo de información de la Empresa	Fallas de Acceso a Archivos, perdida de datos
	La Licencias de los Antivirus no son renovadas inmediatamente	Virus
	Los equipos de cómputo no cuentan con perfiles de acceso ni restricciones para descargas	Utilización de programas no autorizados
	Los Equipos de cómputo permiten el uso de portables	Infección de sistema por uso de portables sin escaneo
	Los usuarios del sistema de información comparten las contraseñas	Manejo inadecuado de contraseñas
	El sistema de información se cae con frecuentemente	Fallas de Acceso a Archivos
	El motor de base de datos es obsoleto	Infiltración
	Los correos institucionales no cuentan con contraseñas de acceso	Acceso Electrónico no autorizado

RED	Existen puntos de acceso a la red física a la vista	Red cableada expuesta a exceso no autorizado
FACTOR HUMANO	varios usuarios tiene acceso al servidor ftp	Intrusión a red interna
	Compartir contraseñas o permisos a terceros	Fraude, hurto de información
	La empresa cuenta con solo un vigilante para la seguridad de toda la empresa	Daños por vandalismo
	No existe mantenimiento al sistema contra incendios	Incendio
	No se realiza capacitación del manejo del sistema de información	Mal manejo de sistemas y Herramientas informáticas
	Dependencia a servicio técnico externo	Fraude, hurto de información
	No existen planes de contingencia	Daño físico irreparable
	No existe documentación políticas de Seguridad	Daño en caso de falla de seguridad

Fuente: Autores del proyecto LKYY

4.2.5 Identificación De Impacto

A nivel de disponibilidad:

Se puede establecer que la infraestructura de red determinada para COMFAORIENTE EPS-S, presenta problemas de Congestión de la Red, en ciertas horas del día donde el tráfico es mayor del que se puede transitar. También cabe mencionar que el servidor perteneciente a COMFAORIENTE EPS-S, presentan insuficiencia de transmisión de datos cuando el volumen de usuarios es elevado.

El sistema de Información SIS_AUDITOR es administrado por su desarrollador, el cual al presentar fallas se requiere de un cambio la presencia del mismo es indispensable.

A nivel de divulgación:

La información es propia y única de COMFAORIENTE EPS-S, por lo tanto su divulgación expone a la Empresa y a sus usuarios, en este caso a los administrativos y usuarios, frente a cualquier situación de violación de la privacidad.

El mayor impacto potencial sería las bases de datos financieras, prestación de servicios, autorizaciones e información personal de la población afiliada a COMFAORIENTE EPS-S

donde quedara expuesta a cualquier individuo ajeno a la empresa ya que se maneja información confidencial de población alto costo, población identificada como ley 1448 (Victimas del Conflicto Armado) y supervivencia lo cual su divulgación puede atentar con la seguridad e integridad de los afiliados por su caracterización.

A nivel de modificación:

Es el nivel de impacto más alto, pues la información de la población afiliada a COMFAORIENTE EPS-S es personal e intransferible; por eso si se llegara a presentar un problema de modificación, generaría problemas de inconsistencia de la información, a nivel de todo el sistema, perdiendo credibilidad y confidencialidad, incluso podría llevar a dejar inútil el sistema.

Así mismo como la integridad de la información en los reportes ante los entes de control, cuya imprecisión puede llevar a sanciones económicas que afectarían el patrimonio de la empresa.

4.2.5 Análisis Cualitativo De Los Riesgos

Teniendo en cuenta la Magnitud de daño de la infraestructura de Comfaoriente eps-s, los datos y el personal contra las amenazas que presenta la dependencia de Sistemas de COMFAORIENTE EPS-S como criminalidad y legalidad, amenazas físicas y negligencia del personal se aplica la siguiente matriz de riesgo Donde,

Tabla 7. Análisis cualitativo

MAGNITUD DE DAÑO		
	INSIGNIFICANTE	1
	BAJO	2
	MEDIANO	3
	ALTO	4

PROBABILIDAD E AMENAZA		
	IMPROBABLE	3
	POSIBLE	6
	PROBABLE	9
	CASI SEGURO	12

RIESGO	VALORACION
BAJO	1-16
MEDIO	17-32
ALTO	33-48

Fuente. Autores del Proyecto LKYY

Por tanto se observa en la Tabla 8 la matriz de riesgos para los sistemas e infraestructura de Comfaoriente Eps-s, donde el Rack, switches, Routers, Servidores y sistemas contraincendios son los más importantes para la empresa, cuya magnitud de daño son los más altos.

Del mismo modo en la Tabla 9 Se observa la matriz de riegos para software y datos, los cuales las bases de datos, el sistema de información, las Backups y los antivirus poseen las más altas magnitudes de daño, teniendo en cuenta la importancia de la información, ya que su perdida atentaría con el funcionamiento y naturaleza de la empresa.

Seguidamente en la Tabla 10 se muestra la matriz de riesgos para personal donde los funcionarios imprescindibles para el correcto funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S y que requieren de sus disposición y disponibilidad 7/24 es el jefe de sistemas y el Ingeniero Desarrollador.

Tabla 8.Matriz Riesgos Con Base A Sistemas E Infraestructura

MATRIZ DE RIESGOS SISTEMAS COMFAORIENTE EPS-S	PROBABILIDAD DE AMENAZA (3,6,9,12)																					
		CRIMINALIDAD Y LEGALIDAD							FISICO				NEGLIGENCIA PERSONAL									
SISTEMAS E INFRAESTRUCTURA	MAGNITUD DE DAÑO (1,2,3,4)	Virus	Infiltracion	Intrusion a red interna	Hurto de Informacion	Hurto fisico	Fraude	Daños por vandalismo	Incendio	Inundacion	Sismo	Falla electrica	Mal manejo de sistemas y Herramientas	Utilizacion de programas no autorizados	Perdida de datos	Infeccion de sistema por uso de portables sin escaneo	Manejo inadecuado de contraseñas	Fallas de Acceso a Archivos	Acceso Electronico no autorizado	Red cableada expuesta a exceso no	Daño en caso de falla de seguridad	Ausencia de documentacion
		9	9	6	6	9	3	3	3	6	9	9	9	3	9	9	9	9	9	9	9	9
Rack	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Router	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Switch	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Firewall	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Servidores	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Equipos de Escritorio	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Portátiles	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Impresoras	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	9	18	18	18	18
Discos duros externos	1	9	9	6	6	9	3	3	3	6	9	9	9	3	9	9	9	9	9	9	9	9
Aire Acondicionado	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Telefonos	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Fuentes de Alimentacion	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Sistema Contra Incendio	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
USB	1	9	9	6	6	9	3	3	3	6	9	9	9	3	9	9	9	9	9	9	9	9

Fuente: Autores del Proyecto LKY

Tabla 9.Matriz Riesgos Software Y Datos

MATRIZ DE RIESGOS SISTEMAS COMFAORIENTE EPS-S	PROBABILIDAD DE AMENAZA (3,6,9,12)																					
		CRIMINALIDAD Y LEGALIDAD							FISICO				NEGLIGENCIA PERSONAL									
SOFTWARE Y DATOS	MAGNITUD DE DAÑO (1,2,3,4)	Virus	Infiltracion	Intrusion a red interna	Hurto de Informacion	Hurto fisico	Fraude	Daños por vandalismo	Incendio	Inundacion	Sismo	Falla electrica	Mal manejo de sistemas y Herramientas	Utilizacion de programas no autorizados	Perdida de datos	Infeccion de sistema por uso de portables sin escaneo	Manejo inadecuado de contraseñas	Fallas de Acceso a Archivos	Acceso Electronico no autorizado	Red cableada expuesta a exceso no	Daño en caso de falla de seguridad	Ausencia de documentacion
		9	9	6	6	9	3	3	3	6	9	9	9	3	9	9	9	9	9	9	9	9
Manual de Procesos y Procedimientos dependencia de Sistemas	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Manual Sistema de Informacion	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Base de datos Facturas	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Base de datos Autorizaciones	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Base de datos de Contratos Red de Servicios	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Base de Datos Basicos Usuarios	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Base de datos Numeros Telefonicos referencia	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Backups	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Correo Electronico	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Pagina web	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Base de datos de Contraseñas	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Chat Interno BIG ANT	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18
Llamadas telefonicas	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Sotfware de aplicación del servidor	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Software de Aplicación de Usuario final	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
herramientas de desarrollo	3	27	27	18	18	27	9	9	9	18	27	27	27	9	27	27	27	27	27	27	27	27
Sistema de Informacion SIS-Auditor	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Antivirus	4	36	36	24	24	36	12	12	12	24	36	36	36	12	36	36	36	36	36	36	36	36
Base de datos de RIPS	2	18	18	12	12	18	6	6	6	12	18	18	18	6	18	18	18	18	18	18	18	18

Fuente: Autores del Proyecto LKYY

Tabla 10.Matriz Riesgos Personal

MATRIZ DE RIESGOS SISTEMAS COMFAORIENTE EPS-S	PROBABILIDAD DE AMENAZA (3,6,9,12)																				
		CRIMINALIDAD Y LEGALIDAD							FISICO				NEGLIGENCIA PERSONAL								
PERSONAL **Fuente: Autores del Proyecto LKYY**	MAGNITUD DE DAÑO (1,2,3,4)	Virus	Infiltracion	Intrusion a red interna	Hurto de Informacion	Hurto fisico	Fraude	Daños por vandalismo	Incendio	Inundacion	Sismo	Falla electrica	Mal manejo de sistemas y Herramientas	Utilizacion de programas no autorizados	Perdida de datos	Infeccion de sistema por uso de portables sin escaneo	Manejo inadecuado de contraseñas	Fallas de Acceso a Archivos	Acceso Electronico no autorizado	Red cableada expuesta a exceso no	Daño en caso de falla de seguridad	Ausencia de documentacion
		9	9	6	6	9	3	3	3	6	9	9	9	3	9	9	9	9	9	9	9	9
Personal Tecnico Informático	2	18	18	**12**	**12**	18	**6**	**6**	**6**	**12**	18	18	18	**6**	18	18	18	18	18	18	18
Ingeniero de Desarrollo	4	36	36	24	24	36	**12**	**12**	**12**	24	36	36	36	**12**	36	36	36	36	36	36	36	36
Jefe de Sistemas	4	36	36	24	24	36	**12**	**12**	**12**	24	36	36	36	**12**	36	36	36	36	36	36	36	36
Limpieza de Dependencia	1	**9**	**9**	**6**	**6**	**9**	**3**	**3**	**3**	**6**	**9**	**9**	**9**	**3**	**9**	**9**	**9**	**9**	**9**	**9**	**9**	**9**
Servicio de Mensajería	1	**9**	**9**	**6**	**6**	**9**	**3**	**3**	**3**	**6**	**9**	**9**	**9**	**3**	**9**	**9**	**9**	**9**	**9**	**9**	**9**	**9**

4.2.6 Contramedidas

Seguidamente de la identificación de riesgos para la dependencia de sistemas COMFAORIENTE EPS en la siguiente tabla se proponen contramedidas para mitigar los riesgos considerados como altos.

Tabla 11. Contramedidas

TIPO	RIESGO	CONTRAMEDIDA	RESPONSABLE
SISTEMAS E INFRAESTRUCTURA	Hurto de Rack	• Instalación de cámaras en la dependencia de sistemas. • Bitácora de acceso personal dependencia de sistemas	• Jefe de Sistemas • Talento humano Y recursos físicos
	Incendio de Rack	• Mantenimiento constante de sistemas contra Incendios	• Talento humano Y recursos físicos
	Perdida del Rack por sismo	• El riesgo se asume	-
	Ausencia de Documentación del cableado del rack	• Realizar la identificación y semaforización del cableado del rack y documentarlo	• Jefe de Sistemas
	Acceso no autorizado al rack	• Bitácora de acceso personal dependencia de sistemas • Instalación de cámaras en la dependencia de sistemas.	• Jefe de Sistemas • Talento humano Y recursos físicos
	Compartir contraseñas a terceros del Router	• Configuración del Router exclusiva de jefe de sistemas. • Elaborar acuerdo confidencialidad de contraseñas	• Jefe de Sistemas • Talento humano Y recursos físicos

	Compartir contraseñas a terceros del Switch	• Configuración del Switch exclusiva de jefe de sistemas. • Elaborar acuerdo confidencialidad de contraseñas	• Jefe de Sistemas • Talento humano Y recursos físicos
	Compartir contraseñas de firewall	• Reducir el acceso al Firewall al jefe de sistemas. • Elaborar acuerdo confidencialidad de contraseñas	• Jefe de Sistemas • Talento humano Y recursos físicos
	Hurto Servidor	• Instalación de cámaras en la dependencia de sistemas. • Bitácora de acceso personal dependencia de sistemas	• Jefe de Sistemas • Talento humano Y recursos físicos
	Incendio de los servidores	• Mantenimiento constante de sistemas contra Incendios	• Talento humano Y recursos físicos
	Daño a los servidores por Sismo	• Implementación de Servidor Espejo • Realizar Backups diariamente y consolidarlas en un sistema de almacenamiento externo	• Jefe de Sistemas
	Daño de los servidores por falla eléctrica	• Realizar mantenimiento preventivo al cableado eléctrico	• Talento humano Y recursos físicos
	Acceso no autorizado a los servidores Daño al sistema contra	• Elaborar acuerdo confidencialidad de contraseñas • Bitácora de acceso personal	• Jefe de Sistemas

	incendios por falla eléctrica	dependencia de sistemas	
	Ausencia de documentación del sistema contra incendios.	• Documentar las conexiones del sistema contra incendios, planos y rutas de evacuación.	• Talento humano Y recursos físicos
	Perdida de base de datos de facturación, autorizaciones y contactos de referencia por incendio	• Mantenimiento constante de sistemas contra Incendios	• Talento humano Y recursos físicos
	Perdida de base de datos de facturación, autorizaciones y contactos de referencia por sismo	• Implementación de Servidor Espejo • Realizar Backups diariamente y Consolidarlas en un sistema de almacenamiento externo	• Jefe de Sistemas
	Perdida de base de datos de facturación, autorizaciones y contactos de referencia por falla Eléctrica	• Implementación de Servidor Espejo • Realizar Backups diariamente y Consolidarlas en un sistema de almacenamiento externo	• Jefe de Sistemas
SOFTWARE Y DATOS	Manipulación de información de facturación autorizaciones, contratación de servicios y datos de usuarios por manejo inadecuado de contraseñas	• Elaborar acuerdo confidencialidad de contraseñas • Requerir que los usuarios cambien la contraseña periódicamente. • especificar una longitud mínima para las contraseñas y	• Jefe de Sistemas

		requerir que la contraseña cumpla con ciertos requisitos de complejidad.	
	Hurto de Backups	• Manejo de Backups exclusivo del jefe de sistemas • Instalación de cámaras en la dependencia de sistemas.	• Jefe de Sistemas • Talento humano Y recursos físicos
	Perdida de Backups por incendio	• Mantenimiento preventivo constante de sistemas contra Incendios	• Talento humano Y recursos físicos
	Perdida de Backups por sismo	• Consolidar Backups en un sistema de almacenamiento externo	• Talento humano Y recursos físicos • Jefe de Sistemas
	Perdida de Backups por falla eléctrica	• Consolidar Backups en un sistema de almacenamiento externo	• Jefe de Sistemas
	Manipulación de Backups por manejos inadecuado de contraseñas	• Custodia y acceso a las Backups exclusivo al jefe de sistemas.	• Jefe de Sistemas
	Documentación de Backups	• Elaborar un manual de Backups donde se registre los pasos a seguir y las fechas de las mismas.	• Jefe de Sistemas

	Acceso al sistema de información por terceros	• Elaborar acuerdo confidencialidad de contraseñas • Requerir que los usuarios cambien la contraseña periódicamente. • Bloquear los equipos de cómputo después de determinado tiempo. • Sistema de detección de intrusos de red y host	• Jefe de Sistemas
	Ingreso al Sistema de Información SIS_AUDITOR por manejo inadecuado de contraseñas.	• Elaborar acuerdo confidencialidad de contraseñas • Bloquear los equipos de cómputo después de determinado tiempo	• Jefe de Sistemas
	Perdida de datos o infección de equipos por virus	• Realizar escaneo programado y actualizaciones periódicas de antivirus.	• Técnico
PERSONAL	Ausencia de documentación de funciones de Ingeniero Sistemas y Desarrollador en la Dependencia.	• Incluir en el manual de procesos y procedimientos las funciones y perfil profesional de cada uno de los funcionarios de la dependencia de sistemas, incluyendo acuerdos de confidencialidad.	• Talento humano Y recursos físicos • Jefe de Sistemas

Fuente. Autores del Proyecto LKYY

4.3. Documentar los parámetros y el desarrollo de la planeación del sistema de gestión de seguridad de la información (SGSI) en la dependencia de sistemas de Comfaoriente EPS-S.

Para el presente objetivo se define el alcance, los objetivos y se diseña el documento de las Políticas de Seguridad de la Información para la Dependencia del área de Comfaoriente EPS. En donde se tomó como referencia la Norma ISO/IEC 27001:2013, donde establece unos lineamientos y principios generales para iniciar, implementar, mantener y mejorar la seguridad de la información de la organización.

4.3.1. Objetivos y alcance del sistema de gestión de seguridad de la información

OBJETIVOS

- Presentar una política de uso adecuado de la tecnología para el procesamiento de la información.

- Mantener la Política de Seguridad de la información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la dependencia del área de sistemas de Comfaoriente EPS para asegurar su nivel de eficacia.

ALCANCE

La presente Política de Seguridad de la Información se realiza en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la dependencia del área de sistemas de Comfaoriente EPS.

Debe ser conocida y cumplida por todo el personal administrativo y operativo del área, tanto para funcionarios internos o externos.

4.3.2 Diseño De Políticas De Seguridad

En su desarrollo se asumieron, los dominios, objetivos de control y los controles los cuales deben ser implementados para mitigar los riesgos encontrados en la empresa.
ANEXO 16(DOMINIOS DE LA NORMA 27001:2013 ANEXO A)

4.3.3 Políticas de Seguridad de la Información

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En la dependencia del área de sistemas de Comfaoriente EPS la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas

como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La Política de Seguridad de la Información de la dependencia de sistemas de Comfaoriente EPS-S se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información del instituto.

Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

Fecha:

Version:1

Propuesta: Autores Del proyecto

Tipo de documento: Políticas de seguridad de la dependencia de sistemas de Comfaoriente EPS-s

POLITICAS DE SEGURIDAD DE LA INFORMACION

- Política de la Organización de la seguridad de la información
- Política de la Seguridad de los recursos humanos
- Política de Gestión de activos
- Política de Control de acceso
- Política de Seguridad física y del entorno
- Política de Seguridad de las operaciones
- Política de Seguridad de las comunicaciones
- Política de Adquisición desarrollo y mantenimiento de los sistemas
- Política de Gestión de incidentes

LÍNEA BASE DE LA POLÍTICA

RESPONSABILIDAD

Es responsabilidad de la dependencia del grupo de sistemas de Comfaoriente eps-s de hacer uso de la Política de Seguridad de la Información, como parte de su manera de gestionar sus servicios, de establecer los procedimientos y todos aquellos lineamientos que garanticen su debido cumplimiento.

CUMPLIMIENTO

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los colaboradores, contratistas, terceras partes violan estas políticas, la dependencia se reserva el derecho de tomar las medidas correspondientes o que esta considere necesarias.

EXCEPCIONES

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por la dependencia del grupo de sistemas de Comfaoriente eps-s, la cual puede requerir autorización. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

Revisión de las políticas para la seguridad de la información.

Las políticas de seguridad de la información se revisarán periódicamente (mínimo una vez por año), o antes, en caso de producirse cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, que puedan afectar su continuidad. La aprobación de las actualizaciones y/o modificaciones, se realizará por parte de un Comité de Seguridad de la Información establecido previamente en la dependencia.

POLITICAS DE SEGURIDAD

POLITICA DE SEGURIDAD LOS RECURSOS HUMANOS

Los trabajadores de la dependencia deben conocer la importancia del correcto uso de las herramientas tecnológicas y sus activos, como bases de datos, equipos de cómputo, comunicaciones, software, documentos, La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes.

Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

CONTROLES:

- Los Empleados y contratistas son responsables de la información entregada para el ejercicio de su función y deberán cumplir con los lineamientos dados por la Entidad y la dependencia, con el propósito de proteger y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

- Los empleados públicos y contratistas no deben suministrar información de la entidad a entes externos sin autorización.

- Los empleados de la dependencia que utilicen recursos informáticos, tiene la responsabilidad de asegurad la integridad, confidencialidad, disponibilidad y confiabilidad de la información que administra, en especial si está protegida por reserva legal o ha sido clasificada como confidencial y/o critica.

- Todo empleado de la dependencia debe abstenerse de ejecutar acciones tendientes a declinar o violar Las Políticas de Seguridad de la Información.

SEGURIDAD FISICA Y DEL ENTORNO

La parte física y del entorno es de una importancia significativa en la dependencia, por eso se pretende velar por la seguridad de la misma para la protección del entorno que nos rodea. En base a lo anterior se crearan una serie de propuestas para impedir accesos no autorizados y evitar daños e interferencias a las sedes e información de la dependencia de grupo de sistemas de Comfaoriente EPS-S.

CONTROLES

- Cada uno de los empleados de la dependencia debe custodiar que toda la información que esta consignada en documentos físicos deben ser protegidas en lugares que dificulten el acceso a personal no autorizado.
- El empleo de escritura en las unidades de DVD/CD, será deshabilitada, salvo autorización del Comité de Seguridad.
- Todos los empleados de la dependencia deben tener presente que no se permite el retiro de equipos de cómputo que contienen información del mismo, sin autorización y conocimiento del comité de seguridad, a fin de llevar a cabo una verificación de la actividad que se realizara y el tipo de información que contiene.
- Las impresoras adquiridas en el establecimiento deben ser aptas para trabajar en red (conectadas a un punto de red y no a un computador), su uso debe realizarse por mínimo 2 personas de la dependencia.
- El comité de seguridad se encargara de mantener seguros los servidores y estaciones de trabajo que contengan la información institucional mediante: o Controles de acceso y seguridad física. o Sistema de vigilancia (Cámaras, alarmas). o Sistema de detección de incendios. o Control de humedad temperatura. o Bajo riesgo de inundación. o Instalación de fuentes de potencia ininterrumpida (UPS)
- Ningún empleado podrá destapar equipos o impresoras para realizar cualquier clase de mantenimiento o instalación de hardware o software, sin una previa autorización.
- Todos los empleados, deben abstenerse de hacer uso de dispositivos de almacenamiento con puertos USB, tarjetas de memoria (SD, MMC, Micro SD, Mini SD Memory Stick, Compact flash1, Micro drive, entre otros).

GESTION DE COMUNICACIONES Y OPERACIONES

La seguridad de la comunicación y las operaciones se encuentran diseñadas para garantizar la seguridad y el respaldo de la información.

CONTROLES

- El jefe de Informática o su encargado, instalará antivirus en los servidores y estaciones de trabajo y configurados para actualizaciones diarias.
- Todo empleado de la dependencia debe evitar el envío de información mediante equipos electrónicos y tecnológicos que a través de sistemas de interconexión inalámbrica permitan la transmisión y almacenamiento de datos, tales como agendas digitales, iPod, iPad, BlackBerry, PDA's, PALMS, equipos electrónicos que contengan sistemas infrarrojos, wireless o bluetooth y celulares inteligentes, entre otros.
- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993.
- El jefe de Informática monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.
- Todo empleado debe abstenerse de hacer uso inadecuado de la red de datos (WAN y LAN) de la dependencia, para obtener, almacenar y difundir en los equipos de cómputo, material pornográfico, mp3, videos y películas comerciales, cadenas de correos no autorizados.
- Las instalaciones de software deben ser aprobadas por el jefe de Informática y en el caso de encontrarse software ilegal en alguna dependencia, será reportado como incidente de seguridad y posteriormente investigado.
- Todo empleado de la dependencia debe abstenerse de realizar actividades que puedan alterar el desempeño de los sistemas de información y por ende generar posibles pérdidas o daños de la misma, como la instalación de software no licenciado, esta conducta genera riesgos, como el ingreso de virus, instalación de software espía, hurto o divulgación no autorizada de la información.
- La dependencia de Sistemas contará con mínimo un cortafuego (Firewall) que prevenga el acceso de intrusos al sistema.
- Todos los empleados de la dependencia deben realizar copias de seguridad de los datos del computador asignado, en forma mensual o en intervalos de tiempo acordes con la necesidad del usuario y de criticidad de la información.
- El jefe de Informática o el encargado, elaborará copias de seguridad semanales y las guardará en sitios bajo llave. Es recomendable que las copias de seguridad se almacenen también en un lugar externo al establecimiento para prevenir pérdida de datos en el caso de una destrucción del establecimiento.
- Cuando el empleado abandone el sitio de trabajo, debe cerrar las aplicaciones que se están ejecutando.

CONTROL DE ACCESOS

El control para el acceso a la información de la dependencia estará dado bajo una serie de directrices que aseguran que la misma no corra ningún riesgo de pérdida.

- La dependencia de sistemas elaborará, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de equipos de cómputo.

- A los empleados y contratistas que laboren en la dependencia y que se les asigne un equipo de cómputo, el director del departamento de sistemas les asignara una cuenta con clave de acceso, la cual tiene definido el perfil de usuario para adicionar, modificar, borrar y consultar información.

- El jefe de Informática, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.
- Cuando un empleado se traslade o se retire del establecimiento, el jefe de dependencia debe informar al jefe de talento humano y este a su vez al departamento de sistemas, con por lo menos un día de antelación, para realizar el correspondiente backup y cambios o eliminación de usuarios.
- La contraseña es personal, por lo tanto no debe ser compartida ni revelada, además deben serán cambiadas periódicamente (Mínimo cada dos meses) y suministradas al Jefe inmediato, cada vez que se haga el cambio.
- El uso del correo electrónico e Internet se prohíbe para fines que no sean institucionales dentro y hacia fuera de la institución.
- Cada empleado debe establecer una contraseña distinta para los servicios utilizados
- Cada empleado de la dependencia debe hacer un uso adecuado del correo, descargar los correos continuamente, archivar o eliminar los correos de las carpetas ya leídos y enviados, descargar la carpeta de mensajes eliminados mínimo de forma semanal.
- La cuenta de correo no debe ser utilizada para enviar o reenviar correos como presentaciones, bromas, video clips, cadenas, pornografía, entre otros. Cuando sean recibidos este tipo de mensajes deberán eliminarse inmediatamente, para evitar la contaminación con posibles virus.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La seguridad de la información depende en gran parte de los controles de seguridad inmersos en las aplicaciones que se manejan.

CONTROLES:

- Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al jefe de Informática, la revisión de incidentes en el manejo de las aplicaciones.
- El jefe de Informática se encargara de actualizar diariamente el software del servidor Web con los parches publicados por el fabricante.
- Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Una adecuada gestión de incidentes le permitirá al establecimiento responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar una base de conocimientos sobre incidentes; evitar en lo posible, incidentes repetitivos.

CONTROLES:

El jefe de Informática de la dependencia ante una incidencia, debe comunicarlo al Comité de Seguridad de la Información y diligenciará el correspondiente formato donde quede consignando los datos de reporte del incidente y de la persona que reportó:

Una vez verificada la incidencia, el jefe de Informática de la dependencia de la Información recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas, qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la empresa

CONCLUSIONES

Después de haber llevado a cabo el reconocimiento de la dependencia de sistemas de Comfaoriente EPS-S a través de una auditoria con la norma 27001: 2013, logramos alcanzar el conocimiento suficiente sobre cómo se encuentra los elementos corporativos como la misión, visión y la estructura orgánica. El estudio realizado demostró que la dependencia carece de la formulación de estos elementos y en algunos casos la inexistencia de los mismos; razón por la cual se realiza una propuesta de misión visión, Objetivos, estructura orgánica e infraestructura Tecnologica.

La segunda fase de la presente investigación permitió formular una identificación de riesgos para la dependencia de Sistemas de Comfaoriente Eps-s con base en la metodología PHVA realizando un reconocimiento de activos, Amenazas, Vulnerabilidades para generar una matriz de riesgos, donde se evidencian los riesgos más altos en los cuales se encuentra expuesta la dependencia.

Del mismo modo se realizó un planteamiento de posibles contramedidas para mitigar dichos riesgos.

Por último se planteó un diseño de las políticas de seguridad de la información para la dependencia. La creación de las políticas de seguridad de la información se basaron en la Norma ISO 27001:2013, tomando los dominios más aplicables a los requerimientos informáticos de la Dependencia de Sistemas de Comfaoriente Eps-s que obtendrá los controles para el mejoramiento de la administración de la información, cumpliendo así los objetivos propuestos del presente proyecto.

RECOMENDACIONES

Socializar el documento de Políticas de Seguridad de la Información con el jefe de sistemas de la dependencia del área de sistemas, de Comfaoriente EPS.

El Jefe de sistemas será el encargado que las políticas de seguridad de la información deben revisarse periódicamente (mínimo una vez por año), o antes, en caso de producirse cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, que puedan afectar su continuidad. La aprobación de las actualizaciones y/o modificaciones, se realizará por parte del Comité de Seguridad de la Información.

El Jefe de Sistemas realizará capacitaciones a todos los empleados y contratistas de la organización de sensibilización, educación y formación adecuada y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función laboral.

BIBLIOGRAFÍA

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. (06 de 04 de 2006). *NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001*. Bogotá: l Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Avila, M. F. (s.f.). *Gestion Empresarial*. Recuperado el 09 de 2015, de Gestion Empresarial: https://gestionempresarial4.wordpress.com/174-2/

Camelo, L. (s.f.). *Seguridad de la Información en Colombia*. Obtenido de Seguridad de la Información en Colombia: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

Dhole, D. (s.f.). *blog-top com*. Obtenido de blog-top com: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

E-CENTRO. (s.f.). *E-CENTRO.* Recuperado el 29 de 11 de 2014, de E-CENTRO: http://centrodeartigo.com/articulos-enciclopedicos/article_80922.html

Gómez Vieites, Á. (s.f.). *wikipedia*. Recuperado el 29 de 2014 de 2014, de wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Juarez, F. M. (s.f.). *normas ISO/IEC 27001*. Obtenido de normas ISO/IEC 27001: http://norma07.blogspot.com.co/2014/09/bienvenidos-todos.html

Pérez, Y. M. (s.f.). *Universidad Francisco de Paula Santander -UFPS.* Obtenido de Universidad Francisco de Paula Santander -UFPS: http://www.ufps.edu.co/ufps/atencionalciudadano/pdf.php?pdf=http://www.ufps.edu.co/ufpsnuevo/archivos/UFPS_Politica_de_seguridad_de_la_informacion.pdf

Públicas, M. d. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Ministerio de Hacienda y Admnistraciones Públicas.

SCRIBD. (s.f.). *https://es.scribd.com.* Recuperado el 28 de 11 de 2014, de https://es.scribd.com: https://es.scribd.com/doc/245012580/Normas-Iso-27000

Velasquez, P. T. (s.f.). *Modulo de Inducción* . Ocaña : www.ufpso.edu.co, 2012.

ANEXOS

Anexo A. Papeles de Trabajo

ARCHIVOS PERMANENTES	NOMENCLATURA
Organigrama de la empresa	**AP-001**
Organigrama de la oficina de sistemas	**AP-002**
Manuales de funciones y procedimientos de la dependencia de grupos de sistemas	**AP-003**
Esquema de distribución de los recursos de computo	**AP-004**
Inventario de recursos de tecnología de información.	**AP-005**
Normas y políticas de seguridad	**AP-006**
Estándares de sistemas	**AP-007**
ARCHIVOS CORRIENTES	**NOMENCLATURA**
Guía de auditoria	**AC-001**
Programa de auditoria	**AC-002**
APLICACIÓN DE PRUEBAS	
Planteamiento prueba N° 1	**AC-003**
Planteamiento prueba N° 2	**AC-004**
Planteamiento prueba N° 3	**AC-005**
Planteamiento prueba N° 4	**AC-006**
Planteamiento prueba N° 5	**AC-007**
Planteamiento prueba N° 6	**AC-008**
Planteamiento prueba N° 7	**AC-010**
Planteamiento prueba N° 8	**AC-011**
Planteamiento prueba N° 9	**AC-012**
Planteamiento prueba N° 10	**AC-013**
Planteamiento prueba N° 11	**AC-014**
Planteamiento prueba N° 12	**AC-015**

Planteamiento prueba N° 13	**AC-016**
Planteamiento prueba N° 14	**AC-017**
Planteamiento prueba N° 15	**AC-018**
Planteamiento prueba N° 16	**AC-019**
Planteamiento prueba N° 17	**AC-020**
Planteamiento prueba N° 18	**AC-021**
Planteamiento prueba N° 19	**AC-022**
SITUACIONES ENCONTRADAS DESPUÉS DE APLICACIÓN DE PRUEBAS	
Situación encontrada Prueba 4	**AC-023**
Situación encontrada Prueba 6	**AC-024**
Situación encontrada Prueba 8	**AC-025**
Situación encontrada Prueba 9	**AC-026**
Situación encontrada Prueba 10	**AC-027**
Situación encontrada Prueba 11	**AC-028**
Situación encontrada Prueba 13	**AC-039**
Situación encontrada Prueba 17	**AC-030**
Situación encontrada Prueba 19	**AC-031**
SITUACIONES RELEVANTES	
Situación relevante prueba 4	**AC-032**
Situación relevante prueba 6	**AC-033**
Situación relevante prueba 8	**AC-034**
Situación relevante prueba 9	**AC-035**
Situación relevante prueba 10	**AC-036**
Situación relevante prueba 11	**AC-037**
Situación relevante prueba 13	**AC-038**
Situación relevante prueba 13	**AC-039**
Situación relevante prueba 17	**AC-040**
Situación relevante prueba 19	**AC-041**

Inventario de Hardware	**HW-042**
Inventario de Software	**SW-043**
Mapa de riesgos	**AC-044**
dictamen	**AC-045**

Anexo B. Programa de Auditoria

PROGRAMA DE AUDITORIA

FASE	DESCRIPCION	ACTIVIDAD	NUM DEL PERSONAL PARTICIPANTE	PERIODO ESTIMADO		DIAS HABILES ESTABLECIDOS	DIAS HOM. EST.
				INICIO	TERMINO		
Recolección de información de la Empresa	En esta fase se solicitara información de la Empresa, al personal directivo. La información será obtenida con la finalidad de apoyar el cumplimiento de los objetivos y el alcance establecido para el desarrollo de la auditoria en la Dependencia de Sistemas. En los papeles de trabajo de auditoría se aclarara la fuente desde donde se	AC1. Recopilar la información de la empresa como: misión, visión, objetivos, procesos entre otros. AC2. Evaluar cada uno de los procesos y subprocesos que maneja la dependencia del grupo de sistemas de Comfaoriente EPS.	4	01/06/2015	03/06/2015	3	3

	ha obtenido la información.						
Realización de pruebas y análisis de los resultados obtenidos	En la fase de realización de pruebas y análisis de sus resultados, se quiere verificar la eficiencia y eficacia del sistema SIS Auditor que maneja la dependencia de sistemas de Comfaoriente EPS.	AC1. Evaluar los sistemas de información que maneja la dependencia de sistemas de Comfaoriente EPS, mediante la utilización de una lista de chequeo AC2. Evaluar el funcionamiento de la dependencia de sistemas por medio de la realización encuestas al personal que labora en esta dependencia. AC3. Análisis de los	4	04/06/2015	06/06/2015	3	3

		resultados arrojados en la lista de chequeo y encuestas aplicadas, mediante tabulación de los mismos.					
Identificación de los Riesgos que exponen la seguridad de la información	En la fase de identificación de Riesgos se pretende verificar la eficiencia y la eficacia del sistema SIS Auditor que maneja la dependencia, en cuanto a la seguridad de la información.	AC1. Diseñar herramientas para la identificación de riesgos: matriz AC2. Aplicación de las herramientas de identificación de riesgos. AC3. Elaborar una valoración cuantitativa y cualitativa de los riesgos.	4	07/06/2015	10/06/2015	3	3

Documentación de los parámetros de planeación.	En esta fase se realizara una documentación a los parámetros que guiara la planeación del sistema de seguridad de la Información (SGSI) en la dependencia de sistemas de Comfaoriente EPS-S	AC1. Identificación de dominios, objetivos de control y controles ajustados a la problemática de la organización AC2. Crear una política de gestión de seguridad de la información.	4	11/06/2015	14/06/2015	3	3
Presentación del dictamen	En esta fase el grupo auditor da a conocer todas las conclusiones después de realizadas las diferentes pruebas sobre el departamento de sistemas de Comfaoriente EPS.	AC1. Presentación del Dictamen sobre la dependencia del grupo de sistemas de Comfaoriente EPS.	4	15/06/2015	15/06/2015	3	3

Anexo C.Guía de Auditoria

GUIA DE AUDITORIA						
Asesoría y Auditoria de Sistemas	Dependencia del Grupo de Sistemas De Comfaoriente EPS-S			FECHA		HOJA
				DIA	MES / AÑO	
REFERENCIA	ACTIVIDAD O FUNCION A EVALUAR	TECNICA O EVALUACIÓN	PONDERACION	CALIFICACION		OBSERVACION
GA.1	AC1. Recopilar la información de la empresa como: misión, visión, objetivos, procesos entre otros.	Solicitar la información de la Empresa para su revisión.				
	AC2. Evaluar cada uno de los procesos y subprocesos que maneja la dependencia del grupo de sistemas de Comfaoriente EPS.	Solicitar los manuales de Procesos y subprocesos al personal encargado. Revisión de los manuales. Se aplicara la matriz de evaluación o lista de chequeo.				

GA.2	AC3. Evaluar los sistemas de información que maneja la dependencia de sistemas de Comfaoriente EPS, mediante la utilización de una lista de chequeo.	Realización de una lista de chequeo al jefe de la Dependencia del Grupo de Sistemas de Comfaoriente ESP-S.			Llevar previamente la lista de chequeo para la aplicación de la misma.
	AC4. Evaluar el funcionamiento de la dependencia de sistemas por medio de la realización encuestas al personal que labora en esta dependencia.	Aplicación de encuestas a los funcionarios que laboran en la dependencia del Grupo de Sistemas de Comfaoriente ESP.S.			Llevar previamente las encuestas para la aplicación de la mismas.
	AC5. Análisis de los resultados arrojados en la lista de chequeo y encuestas aplicadas, mediante tabulación de los mismos. Chequeo y encuestas aplicadas, mediante tabulación de los mismos.	Realizar tabulación gráfica de los resultados obtenidos en la lista de Chequeo y encuestas			

GA.3	AC6. Diseñar herramientas para la identificación de riesgos: matriz	Se aplicara la matriz de evaluación o lista de chequeo.			Las pruebas las debe realizar al auditor
	AC7. Evaluar la seguridad, confiabilidad y los respaldos con los que cuenta la dependencia para salvaguardar la información.	Aplicación de las herramientas de identificación de riesgos.			
	AC8. Elaborar una valoración cuantitativa y cualitativa de los riesgos.	Mediante la aplicación de encuestas al personal que labora en la Dependencia de Sistemas.			

GA.4	AC9. Identificación de dominios, objetivos de control y controles ajustados a la problemática de la organización	Revisión de la Norma Iso 27001 como guía para la identificación de estos dominios y objetivos de control.			
	AC10. Crear una política de gestión de seguridad de la información.	De acuerdo a las necesidades de la seguridad de la información en la Dependencia de Sistemas y los dominios y Objetivos de control establecidos se creara esta política de seguridad para la Empresa.			

GA.5	AC11. Preparación del Dictamen				Se darrollara al finalizar la auditoria.

Anexo D. Pruebas realizadas a la dependencia de Sistemas de Comfaoriente EPS-S

PRUEBAS REALIZADAS DEPENDENCIA GRUPO DE SISTEMAS

PLANTEAMIENTO PRUEBA No.1			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta procedimientos de seguridad.			
Objetivo	Verificar las medidas que tiene la dependencia frente a la seguridad del área.		
Tipo De Prueba	Cumplimiento __x__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Cuestionario. Se realiza la observación y verificación Se realiza la verificación de los controles, procedimientos.		
Recursos	Observación, documentación, cuestionario		
RESULTADOS			
Hallazgos	Se encontraron que existen controles y procedimientos de seguridad.		
Recomendaciones			
Fecha	4/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.2			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con un documento donde se especifique las funciones y obligaciones del personal.			
Objetivo	Verificar el documento de funciones.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad _x___
Procedimiento	Cuestionario. Se realiza la observación y verificación		
Recursos	Observación, documentación, cuestionario		
RESULTADOS			
Hallazgos	Se realizó una revisión de la existencia del documento de funciones.		
Recomendaciones			
Fecha	4/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda		

	Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.3			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas tiene definido procedimientos para las copias de seguridad y recuperación de datos.			
Objetivo	Verificar los procedimientos de copia de seguridad.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad _x___
Procedimiento	Cuestionario. Se realiza la observación y verificación		
Recursos	Observación, cuestionario.		
RESULTADOS			
Hallazgos	Se cuentan con procedimientos de copias de seguridad.		
Recomendaciones	Ninguna.		
Fecha	4/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.4			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con todo l o relacionado a contraseñas en el grupo de trabajo.			
Objetivo	Verificar la utilización de contraseñas, usuarios autorizados, procedimientos de asignación o distribución de contraseñas, sabe de contraseñas con encriptación, documentos de seguridad de contraseña, vigencia de contraseñas.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad __X__
Procedimiento	Cuestionario Empleado Se realiza la observación y verificación		
Recursos	Observación, documentación, cuestionario		
RESULTADOS			

Hallazgos	Se realizó una revisión de la existencia y la eficacia del control de acceso en cuanto a contraseñas
Recomendaciones	Se recomienda contraseñas con encriptación, manejar periodo de licencias para contraseñas y establecer un documento de seguridad donde los empleados guarden su contraseña.
Fecha	4/06/2015
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.5			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con seguridad en mensajería electrónica.			
Objetivo	Verificar las formas de seguridad de mensajería.		
Tipo De Prueba	Cumplimiento __x__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Cuestionario. Se realiza la observación y verificación		
Recursos	Observación, cuestionario		
RESULTADOS			
Hallazgos	Se realizó una revisión de mensajería y formas de seguridad.		
Recomendaciones	Ninguna.		
Fecha	4/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.6			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con seguridad respecto a sus proveedores.			
Objetivo	Verificar la seguridad respecto a proveedores.		
Tipo De Prueba	Cumplimiento __x__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Cuestionario. Se realiza la observación y verificación		
Recursos	Observación, documentación, cuestionario		
RESULTADOS			
Hallazgos	Se evidencio que no se encuentra establecido un procedimiento de seguridad en cuanto a proveedores en la dependencia de sistemas.		
Recomendaciones	Se recomienda establecer procedimientos de seguridad en cuanto a los proveedores que tiene la dependencia.		
Fecha	4/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.7			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con todo l o requerido en cuanto a seguridad de bases de datos.			
Objetivo	Verificar copias de seguridad, roles de usuario, administrador de controles de usuario, gestión de perfiles, gestión de accesos a instancias, las instancias cuentan con acceso restringido, renovación de claves de acceso a la base de datos, diseño físico o lógico, diccionario de datos, copia de seguridad en cuanto a repositorio para el entorno de su desarrollo, seguridad con equipos auxiliares, comunicación con el administrador para restablecimiento de bases de datos, plan de contingencia.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad __X__
Procedimiento	Cuestionario. Se realiza la observación y verificación		
Recursos	Observación, documentación, cuestionario		
RESULTADOS			

Hallazgos	Se evidencia la falta de renovación de claves, diccionario de datos, encriptación de las copias de seguridad y procedimientos para dar de baja a un usuario.
Recomendaciones	Se recomienda establecer la renovación de claves para los usuarios de las base de datos, crear un diccionario de datos, que las copias sean encriptados en algunos casos, si es el caso establecer un procedimiento para dar de baja a un usuario.
Fecha	4/06/2015
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.8			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas existen controles de seguridad en cuanto a redes de comunicación.			
Objetivo	Verificar la existencia del controles		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Aplicar cuestionario.		
Recursos	Cuestionario, verificación.		
RESULTADOS			
Hallazgos	Se realizó una revisión y se evidencio la inexistencia del código de colores en las redes, no cuentan con dispositivos para la expansión de señal de red, no existe un control para acceder a los dispositivos y cableado, no se realizan análisis de vulnerabilidades y ataques.		
Recomendaciones	Se recomienda establecer el código de colores, si en dado de ser necesario tener en reserva un conmutador de red para la expansión de señal, y establecer un control para el acceso a los dispositivos y cableado, desarrollar los análisis de vulnerabilidades de la red, y establecer grupos de servicios separados por redes.		
Fecha	4/06/2015		

Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.9			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar que los mecanismos de seguridad física son los necesarios.			
Objetivo	Verificar los mecanismos de seguridad.		
Tipo De Prueba	Cumplimiento ____	Sustantiva _X___	Doble Finalidad ____
Procedimiento	Verificar mecanismos. Verificar registros de ingresos.		
Recursos	Cuestionario, observación		
RESULTADOS			
Hallazgos	No cuenta con sitios restringidos ni se lleva un registro de las personas que ingresan al área.		
Recomendaciones	Establecer lugares de acceso restringido en el área, y desarrollar un registro de las personas que ingresan al área.		
Fecha	5/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.10			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Grupo de Sistemas cuenta con la seguridad necesaria para los equipos de cómputo.			
Objetivo	Verificar la protección de los equipos de cómputo..		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Escoger 1 equipo al azar. Revisar		
Recursos	Cuestionario, verificación.		
RESULTADOS			
Hallazgos	Se evidencio que cuando los equipos son removidos del área no		

	cuenta con medidas de seguridad establecidas.
Recomendaciones	Establecer un formato cuando los equipos son removidos del área, desarrollar un control cuando estos se encuentren fuera del área en cuanto a seguridad o que medidas deben seguir
Fecha	5/06/2015
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.11			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: comprobar la seguridad de la información y procesos de soporte.			
Objetivo	Verificar la seguridad de la información y proceso de soporte.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad ____
Procedimiento	Solicitar el documento a la EPS.		
Recursos	Observación, documentación.		
RESULTADOS			
Hallazgos	Se encontró que la dependencia de Sistemas, no cuenta con un documento donde se especifiquen la información de nuevos sistemas.		
Recomendaciones	Se recomienda mantener un documento de especificaciones de nuevos sistemas.		
Fecha	5/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.12			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Comprobar si la dependencia Comfaoriente EPS-S cuenta con medios de almacenamiento, para guardar información.			
Objetivo	Verificar si existen medios de almacenamiento.		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Verificar donde se almacena la información.		
Recursos	cuestionario		
RESULTADOS			
Hallazgos	Se encontraron registros diarios de las copias realizadas de parte del jefe del grupo de sistemas.		
Recomendaciones	Ninguna.		
Fecha	5/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.13			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Verificar documentación de los procesos que se manejan en el grupo de sistemas Comfaoriente EPS-S.			
Objetivo	Verificar la existencia de los controles de los diferentes procesos y actualización permanente de la documentación en la dependencia grupo de Sistemas Comfaoriente EPS-S.		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Verificar que se manejen los procesos de Afiliación y registro, de Sistemas. Confirmar que estén funcionando correctamente los programas en función de la documentación de los procesos.		
Recursos	Cuestionario		
RESULTADOS			
Hallazgos	Se encontraron manuales de los procesos, pero no se encuentran actualizados.		
Recomendaciones	Cada vez que se realice un cambio, se deben actualizar los manuales.		

Fecha	5/06/2015
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.14			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
PRUEBA: Existen medios por los cuales se recibe la información.			
Objetivo	Verificar la existencia de canales por los cuales se recibe la información.		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Solicitar el ingreso al sistema de alguno de los empleados. Verificar que pueda acceder a páginas gubernamentales, afiliados. Verificar el uso de correo.		
Recursos	Inspección, cuestionario.		
RESULTADOS			
Hallazgos	Se encontró que en la dependencia si cuenta con canales de trasferencia de información.		
Recomendaciones	Ninguna.		
Fecha	5/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.15			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
Prueba: Verificar si existen bitácoras en el Sistema de Información, y si estas reportan los accesos, los errores y modificaciones importantes.			
Objetivo	Verificar la existencia de las bitácoras.		
Tipo De Prueba	Cumplimiento __X__	Sustantiva ____	Doble Finalidad ____
Procedimiento	Verificar los registros /var/log para observar la actividad. Verificar el sistema de monitoreo.		
Recursos	Cuestionario, observación		
RESULTADOS			
Hallazgos	Se encontraron bitácoras del sistema donde se reportan todos los eventos que ocurren.		
Recomendaciones	Ninguna.		
Fecha	6/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.16			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
Prueba: Verificar que la política de acceso a internet, solo permita el ingreso al chat y correo de la empresa.			
Objetivo	Verificar la existencia de los controles en el acceso al sistema.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad __X__
Procedimiento	Revisar que se pueda ingresar al correo, y a otras funciones que ofrece la red.		
Recursos	Cuestionario, observación.		
RESULTADOS			
Hallazgos	Se encontró que la empresa cuenta con servicio de correo, y paginas a las cuales puede ingresar, solo para el tránsito de la información.		
Recomendaciones	Ninguna.		
Fecha	6/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda		

	Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.17			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
Prueba: Existen controles de software que permitan llevar un seguimiento de los cambios del sistema.			
Objetivo	Verificar la existencia de los controles en el acceso al sistema.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad __X__
Procedimiento	Comprobar si existe documentación de las versiones hechas al software.		
Recursos	Documentación		
RESULTADOS			
Hallazgos	Se encontró que existe documentación de versiones, pero que no están actualizadas.		
Recomendaciones	Actualizar el formato de control de cambios.		
Fecha	6/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

PLANTEAMIENTO PRUEBA No.18			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
Prueba: Verificar programas instalados.			
Objetivo	Verificar que todos los programas instalados en los equipos de cómputo tengan las licencias respectivas y los permisos por parte del área de sistemas.		
Tipo De Prueba	Cumplimiento _X___	Sustantiva ____	Doble Finalidad ____
Procedimiento	Revisar los programas instalados en los equipos. Solicitar las licencias respectivas de cada uno.		
Recursos	Documentación de instalación, cuestionario.		
RESULTADOS			
Hallazgos	Se encontró que en todos los equipos, los programas cuentan con sus respectivas licencias.		

Recomendaciones	Ninguna.
Fecha	6/06/2015
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

PLANTEAMIENTO PRUEBA No.19			
GRUPO SISTEMAS COMFAORIENTE EPS-S			
Prueba: Existen problemas críticos dentro del área de sistemas.			
Objetivo	Verificación de la conexión del SIS-AUDITOR en caso de presentar caídas o fallos.		
Tipo De Prueba	Cumplimiento ____	Sustantiva ____	Doble Finalidad __X__
Procedimiento	Solicitar a un empleado Autorizado a que ingrese al SIS-AUDITOR. Revisar la conexión del SIS-AUDITOR, después de haber ingresado al sistema. Revisar la información que se guarda en el SIS-AUDITOR.		
Recursos	Inspección.		
RESULTADOS			
Hallazgos	Se encontró que existen fallos de conexión en raras ocasiones, pero no hay pérdida de información.		
Recomendaciones	Revisar la topología de Red con la cuenta el área de Sistemas.		
Fecha	6/06/2015		
Elaborado Por	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

Anexo E. Situaciones Encontradas

SITUACIONES ENCONTRADAS					
PRUEBA No. 4					
Empresa		**Área auditada**	**Día**	**Mes**	**Año**
COMFAORIENTE EPS-S		GRUPO DE SISTEMAS	5	06	2015
Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
024	Verificar la utilización de contraseñas, usuarios autorizados, procedimientos de asignación o distribución de contraseñas, sabe de contraseñas con encriptación, documentos de seguridad de contraseña, vigencia de contraseñas.	Al momento de la verificación de contraseñas, se pudo evidenciar que hace faltan cierto criterios sobre estas como encriptación, documentos de seguridad, y vigencia de la misma.	Se recomienda contraseñas con encriptación, manejar periodo de licencias para contraseñas y establecer un documento de seguridad donde los empleados guarden su contraseña.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas
Elaboró por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández			Aprobado por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		
SITUACIONES ENCONTRADAS					

PRUEBA No. 6

Empresa	Área auditada	Día	Mes	Año
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	4	06	2015

Ref.	Situación	Causas	Solución	Fecha de solución	Responsable
025	Verificación de seguridad respecto a proveedores.	No existencia de procedimientos de seguridad en cuanto a proveedores.	Se recomienda establecer procedimientos de seguridad en cuanto a los proveedores que tiene la dependencia.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth ContrerasHernández

SITUACIONES ENCONTRADAS						
PRUEBA No. 8						
Empresa		**Área auditada**		**Día**	**Mes**	**Año**
COMFAORIENTE EPS-S		GRUPO DE SISTEMAS		4	06	2015

Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
026	Verificación controles en las redes.	Inexistencia del código de colores en las redes, no cuentan con dispositivos para la expansión de señal de red, no existe un control para acceder a los dispositivos y cableado, no se realizan análisis de vulnerabilidades y ataques.	Se recomienda establecer el código de colores, y plasmarlo en un documento para el área, si en dado de ser necesario tener en reserva un conmutador de red para la expansión de señal, y establecer un control para el acceso a los dispositivos y cableado, desarrollar los análisis de vulnerabilidades de la red, y establecer grupos de servicios separados por redes.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

SITUACIONES ENCONTRADAS					
PRUEBA No. 9					
Empresa	**Área auditada**	**Día**	**Mes**	**Año**	
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	6	06	2015	
Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
027	Verificación de mecanismos de seguridad.	Inexistencia de sitios restringidos y falta de controles para el ingreso al área.	Establecer lugares de acceso restringido en el área, y desarrollar un registro de las personas que ingresan al área. Todo quede plasmado en un documento.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas
Elaboró por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández			Aprobado por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

SITUACIONES ENCONTRADAS					
PRUEBA No. 10					
Empresa		**Área auditada**	**Día**	**Mes**	**Año**
COMFAORIENTE EPS-S		GRUPO DE SISTEMAS	5	06	2015

Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
028	Remoción de equipos del área de trabajo.	Se evidencio que cuando los equipos son removidos del área no cuenta con medidas de seguridad establecidas.	Establecer un formato cuando los equipos son removidos del área, desarrollar un control cuando estos se encuentren fuera del área en cuanto a seguridad o que medidas deben seguir	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

SITUACIONES ENCONTRADAS					
PRUEBA No. 11					
Empresa		**Área auditada**	**Día**	**Mes**	**Año**
COMFAORIENTE EPS-S		GRUPO DE SISTEMAS	5	06	2015

Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
029	Seguridad de la información y soporte	Se encontró que la dependencia de Sistemas, no cuenta con un documento donde se especifiquen la información de nuevos sistemas.	Se recomienda mantener un documento de especificaciones de nuevos sistemas.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth ContrerasHernández

SITUACIONES ENCONTRADAS					
PRUEBA No. 13					
Empresa	**Área auditada**	**Día**	**Mes**	**Año**	
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	5	06	2015	
Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
030	Verificación de documentos.	Se encontraron manuales de los procesos, pero no se encuentran actualizados.	Se recomienda que cada vez que se realice un cambio, se deben actualizar los manuales.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas
Elaboró por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández			Aprobado por Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández		

SITUACIONES ENCONTRADAS					
PRUEBA No. 17					
Empresa	**Área auditada**	**Día**	**Mes**	**Año**	
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	6	06	2015	

Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
031	Verificación de documentos de control de software	Se encontró que existe documentación de versiones, pero que no están actualizadas.	Se recomienda Actualizar el formato de control de cambios.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

SITUACIONES ENCONTRADAS					
PRUEBA No. 19					
Empresa	**Área auditada**	**Día**	**Mes**	**Año**	
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	6	06	2015	

Ref.	**Situación**	**Causas**	**Solución**	**Fecha de solución**	**Responsable**
032	Verificación conexión del SIS-AUDITOR en caso de fallas.	Se encontró que existen fallos de conexión en raras ocasiones, pero no hay pérdida de información.	Se recomienda Revisar la topología de Red con la cuenta el área de Sistemas.	Solo se establecerá cuando se realice un comité.	Jefe del Grupo de Sistemas

Elaboró por	Aprobado por
Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández	Vianny Karina Buitrago Sepúlveda Yorman José Márquez Fuentes Yeinny Yohana Acosta Vergel Leidy Lisbeth Contreras Hernández

Anexo F. Situaciones Relevantes

SITUACIONES RELEVANTES					
PRUEBA No. 4					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		4	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
033	Verificar la utilización de contraseñas, usuarios autorizados, procedimientos de asignación o distribución de contraseñas, sabe de contraseñas con encriptación, documentos de seguridad de contraseña, vigencia de contraseñas.	Al momento de la verificación de contraseñas, se pudo evidenciar que hace faltan cierto criterios sobre estas como encriptación, documentos de seguridad, y vigencia de la misma.	Se recomienda contraseñas con encriptación, manejar periodo de licencias para contraseñas y establecer un documento de seguridad donde los empleados guarden su contraseña.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA		VIANNY KARINA BUITRAGO SEPULVEDA
YORMAN J. MARQUEZ FUENTES		YORMAN J. MARQUEZ FUENTES
YEINNY Y. ACOSTA VERGEL		YEINNY Y. ACOSTA VERGEL
LEIDY L. CONTRERAS HERNANDEZ		LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES

PRUEBA No. 6

EMPRESA	AREA AUDITADA	DIA	MES	AÑO
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	4	06	2015

Ref.	Situaciones	Causas	Solución
034	Verificación de seguridad respecto a proveedores.	No existencia de procedimientos de seguridad en cuanto a proveedores.	Se recomienda establecer procedimientos de seguridad en cuanto a los proveedores que tiene la dependencia.

Elaboró		Aprobó
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 6					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		4	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
035	Verificación de seguridad respecto a proveedores.	No existencia de procedimientos de renovación de claves y diccionario de datos para las bases de datos. No existencia de encriptación en las copias de seguridad. No establecimiento de procedimientos para dar de baja a un usuario.	Se recomienda establecer la renovación de claves para los usuarios de las base de datos, crear un diccionario de datos, que las copias sean encriptados en algunos casos, si es el caso establecer un procedimiento para dar de baja a un usuario, y que todo quede plasmado en un documento que lo acredite.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 8					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		4	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
036	Verificación controles en las redes.	Inexistencia del código de colores en las redes, no cuentan con dispositivos para la expansión de señal de red, no existe un control para acceder a los dispositivos y cableado, no se realizan análisis de vulnerabilidades y ataques.	Se recomienda establecer el código de colores, y plasmarlo en un documento para el área, si en dado de ser necesario tener en reserva un conmutador de red para la expansión de señal, y establecer un control para el acceso a los dispositivos y cableado, desarrollar los análisis de vulnerabilidades de la red, y establecer grupos de servicios separados por redes.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 9					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		5	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
037	Verificación de mecanismos de seguridad.	Inexistencia de sitios restringidos y falta de controles para el ingreso al área.	Establecer lugares de acceso restringido en el área, y desarrollar un registro de las personas que ingresan al área. Todo quede plasmado en un documento.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA		VIANNY KARINA BUITRAGO SEPULVEDA
YORMAN J. MARQUEZ FUENTES		YORMAN J. MARQUEZ FUENTES
YEINNY Y. ACOSTA VERGEL		YEINNY Y. ACOSTA VERGEL
LEIDY L. CONTRERAS HERNANDEZ		LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 10					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		5	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
038	Remoción de equipos del área de trabajo.	Se evidencio que cuando los equipos son removidos del área no cuenta con medidas de seguridad establecidas.	Establecer un formato cuando los equipos son removidos del área, desarrollar un control cuando estos se encuentren fuera del área en cuanto a seguridad o que medidas deben seguir

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA		VIANNY KARINA BUITRAGO SEPULVEDA
YORMAN J. MARQUEZ FUENTES		YORMAN J. MARQUEZ FUENTES
YEINNY Y. ACOSTA VERGEL		YEINNY Y. ACOSTA VERGEL
LEIDY L. CONTRERAS HERNANDEZ		LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 11					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		5	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
039	Seguridad de la información y soporte	Se encontró que la dependencia de Sistemas, no cuenta con un documento donde se especifiquen la información de nuevos sistemas.	Se recomienda mantener un documento de especificaciones de nuevos sistemas.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES					
PRUEBA No. 13					
EMPRESA	**AREA AUDITADA**		**DIA**	**MES**	**AÑO**
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS		5	06	2015

Ref.	**Situaciones**	**Causas**	**Solución**
040	Verificación de documentos.	Se encontraron manuales de los procesos, pero no se encuentran actualizados.	Se recomienda que cada vez que se realice un cambio, se deben actualizar los manuales.

Elaboró		**Aprobó**
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES

PRUEBA No. 17

EMPRESA	AREA AUDITADA	DIA	MES	AÑO
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	6	06	2015

Ref.	Situaciones	Causas	Solución
041	Verificación de documentos de control de software.	Se encontró que existe documentación de versiones, pero que no están actualizadas.	Se recomienda Actualizar el formato de control de cambios.

Elaboró		Aprobó
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

SITUACIONES RELEVANTES

PRUEBA No. 19

EMPRESA	AREA AUDITADA	DIA	MES	AÑO
COMFAORIENTE EPS-S	GRUPO DE SISTEMAS	6	06	2015

Ref.	Situaciones	Causas	Solución
042	Verificación conexión del SIS-AUDITOR en caso de fallas.	Se encontró que existen fallos de conexión en raras ocasiones, pero no hay pérdida de información.	Se recomienda Revisar la topología de Red con la cuenta el área de Sistemas.

Elaboró		Aprobó
VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ		VIANNY KARINA BUITRAGO SEPULVEDA YORMAN J. MARQUEZ FUENTES YEINNY Y. ACOSTA VERGEL LEIDY L. CONTRERAS HERNANDEZ

Anexo G.Informe de Auditoria

ASESORIA Y AUDITORIA DE SISTEMAS

Cúcuta a 7 de Junio del 2015

Comfaoriente EPS-S
Informe Auditoria

Una vez realizada la auditoria pasiva a la dependencia de Sistemas de COMFAORIENTE EPS-S evaluando algunos aspectos siguiendo la norma 27001:2013 tales como: Red, Seguridad física, Seguridad lógica, Controles de accesos al software que maneja la dependencia, Controles del sitio web que maneja la dependencia, Planes de contingencia y procedimientos de respaldo de la información se evidenció que:

- Del análisis del negocio que se hizo previamente se observó que la dependencia no cuenta con una estructura como la de organigrama por tanto se recomienda realizar su diseño. (Los autores de proyecto plantean el diseño el cual esta anexo.)

Del mismo modo se recomienda:

- Adquisición de un nuevo antivirus para los equipos de la dependencia.
- Creación de los inventarios de hardware y de software así como la ejecución de actualizaciones programadas.
- Actualización de los controles de cambios del sistema de Información.
- Diseño del proceso de segmentación de la red, incluyendo cambios que se puedan presentar en la topología.
- Actualización del plan de contingencia para evitar futuros inconvenientes en caso de presentarse alguna emergencia y puedan ocasionar problemas legales.
- Implementar un sistema para el registro de las personas que ingresan a la dependencia.

Observaciones	Recomendación
Del análisis del negocio que se hizo previamente se observó que la dependencia no cuenta con una estructura como la de organigrama.	Recomendación diseñar una. (el grupo le planteara un diseño de organigrama para la dependencia).

No cuenta con misión, visión y Objetivos	Establecer una para la dependencia.(el grupo presentara una propuesta dentro del marco de su trabajo)
Se observó que los equipos de la dependencia carecen de un buen antivirus.	Adquisición de un nuevo antivirus para los equipos de la dependencia.
No se encuentran establecidos inventarios de hardware y software.	Creación de los inventarios de hardware y de software así como de sus constantes actualizaciones.
Se encontraron controles de cambios pero desactualizados.	Actualización de los controles de cambios del sistema de Información.
La dependencia no cuenta con un diseño de proceso de segmentación ni topología de red.	Diseño del proceso de segmentación de la red, incluyendo cambios que se puedan presentar en la topología.(el grupo presentara una propuesta sobre la topología dentro del marco de su trabajo).
Se encontró un plan de contingencia desactualizado.	Actualización del plan de contingencia para evitar futuros inconvenientes en caso de presentarse alguna emergencia y puedan ocasionar problemas legales.
Se observó que no hay un control de Ingreso para las personas que ingresan a la dependencia.	Se recomienda tener un sistema para el registro de las personas que ingresan a la dependencia.

Este dictamen está destinado para ser utilizado según estime conveniente de acuerdo a su criterio y aclaramos que esta se realizó con fines educativos, y así ofrecer un aporte al mejoramiento del servicio que brinda la dependencia grupo de sistemas de Comfaoriente EPS-S.

Atentamente,

Auditores,

Yeinny Yohana Acosta Vergel
Vianny Karina Buitrago Sepúlveda
Leidy Lisbeth Contreras Hernández
Yorman José Márquez Fuentes

Anexo H. Propuesta Misión Dependencia Sistemas Comfaoriente EPS-S

Proponemos la siguiente.

Misión propuesta: cumplir con los procesos organizados, confiables mediante la utilización de las tecnologías de la información y herramientas tecnológicas apropiadas con las cuales se puedan optimizar de una manera segura y eficiente los procesos y servicios ofrecidos a los usuarios.				
#	CRITERIOS	PREGUNTA	SI	NO
1	Clientes	Quiénes son los clientes?	X	
2	Productos y servicios.	¿cuáles son los servicios o productos más importantes'	X	
3	Mercados	¿Compite geográficamente?	X	
4	Tecnología	¿Cuál es la tecnología básica?		
5	Preocupación por supervivencia, crecimiento y rentabilidad.	¿Cuál es la actitud de la organización en relación a metas económicas?	X	
6	Filosofía	¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización?	X	
7	Concepto de la misma	¿Cuáles son las ventajas competitivas claves?	X	
8	Preocupación por la imagen publica	¿Cuál es la imagen pública a que aspira?, ¿Es responsable socialmente, ante la comunidad y el medio ambiente?	X	
9	Preocupación por los empleados	¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés?	X	

Anexo I. Propuesta Visión

Visión propuesta: Ser un área con principios y valores, innovadora y de un buen manejo de la información que allí es suministrada enfocada a los servicios de la caja de compensación para el beneficio del sector salud conservando el reconocimiento a nivel departamental, regional y nacional.			
#	CRITERIOS	SI	NO
1	Orientado al futuro incluso en su redacción		x
2	Es integradora	X	
3	Es corta	X	
4	Es positiva y alentadora.	X	
5	Es realista y posible.	X	
6	Es consistente con los principios y valores de la organización	X	
7	Orienta la transición de los que es a lo que debe llegar a ser	X	
8	Expresa claramente los logros que se esperan en el periodo	X	
9	Cubre todas las áreas actuales y futuras de la organización	X	
10	Está redactada en términos que signifiquen acción	X	
11	Tienen fuerza e impulsa a la acción	X	
12	Contiene el futuro visualizado	X	
13	Es el sueño alcanzable a largo plazo	X	

Anexo J. Cuestionario Políticas de Seguridad de la Información

Cuestionario Politicas de Seguridad de la Informacion				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Políticas de seguridad	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Medidas, controles, procedimientos, normas y estándares de seguridad Contraseñas Autorización del personal
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
1. ¿Existen medidas, controles, procedimiento o estándares de seguridad?			
2. ¿existe un documento donde se encuentre especificado las funciones y obligaciones del personal?			
3. ¿Existen procedimientos de realización de copias de seguridad y de la recuperación de datos?			
4. ¿Existe un periodo máximo de utilización de las contraseñas?			
5. ¿Existe una relación de usuarios autorizados para acceder a los sistemas e incluye los accesos permitidos a los cuales debes acceder?			
6. ¿Existen procedimientos de asignación o distribución de contraseñas?			
7. ¿El sistema de autenticación de usuario guarda las			

contraseñas con encriptación?			
8. ¿Existe un documento de seguridad donde las personas guardan su contraseña			
9. El sistema esta habilitadas para todas las cuentas de usuario las opciones que permiten establecer: Un número máximo de intentos de conexión. Un periodo máximo de vigencia para la contraseña.			
10. existen medidas de seguridad en cuanto a la mensajería electrónica			
11. existen documento de confidencialidad y divulgación			
12. existen tratamientos de seguridad de acuerdo con los proveedores			
13. existen cadenas de suministro entre la tecnología de información y comunicación			
total			

Anexo K. Cuestionario de control de base de datos

Cuestionario de control de base de datos				
	Auditoria de seguridad de la Información	Proceso: Norma ISO 27001:2013		
	Bases de Datos	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad de la Información Bases de Datos Seguridad de la Información
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?			
Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?			
Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?			
Son gestionados los perfiles de estos usuarios por el administrador?			
Son gestionados los accesos a las instancias de la Base de Datos?			
Las instancias que contienen el repositorio, tienen acceso restringido?			
Se renuevan las claves de los usuarios de la Base de Datos?			
Posee la base de datos un diseño físico y lógico?			
Posee el diccionario de datos un diseño físico y lógico?			
Existe una instancia con copia del Repositorio para el entorno de desarrollo?			
Las copias de seguridad se efectúan diariamente?			
Las copias de seguridad son encriptados?			
Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?			
Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?			
En caso de que el equipo principal sufra una avería, existen equipos auxiliares?			
Cuando se necesita restablecer la base de datos, se le comunica al administrador?			
Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?			
Es eliminada la cuenta del usuario en dicho procedimiento?			
Hay algún procedimiento para dar de baja a un usuario?			
Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			
TOTAL			

Anexo L.Cuestionario de Redes y Comunicaciones

Cuestionario de Redes y Comunicaciones				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Redes y Comunicaciones	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Evaluación Infraestructura de redes de comunicación Instalación y diseño de redes
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se gestiona la infraestructura de la red inalámbrica en base a los recursos de radiofrecuencia de los clientes?			
¿Los enlaces de la red se testean frecuentemente?			
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?			
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?			
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?			
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?			
¿Las direcciones IP´S de los equipos de cómputo son implementadas de forma fija?			

¿Cuentan con conmutadores en red, para la expansión de redes locales?			
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?			
Cuenta con dispositivos para la regulación del voltaje?			
Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos			
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?			
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?			
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?			
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?			
En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y Encontrar posibles fallas?			
Cuentan con administración interna de la red es decir, ¿cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?			
Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?			
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?			
¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?			
Existen grupos de servicios de información, usuarios y sistemas de información que se separen por redes?			

Anexo M. Cuestionario de Seguridad física y del entorno

Cuestionario de Seguridad física y del Entorno				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Física y del Entorno	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad física
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se tienen lugares de acceso restringido?			
¿Se poseen mecanismos de seguridad para el acceso a estos lugares?			
¿Tiene medidas implementadas ante la falla del sistema de seguridad?			
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?			
¿Se tiene un registro de las personas que ingresan a las instalaciones?			
TOTAL			

Anexo N.Cuestionario de Seguridad de Equipos

Cuestionario de Seguridad de Equipos				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Equipos	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	equipos
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Los equipos están ubicados y protegidos para reducir las amenazas y peligros del entorno?			
¿Los equipos cuentan con protección contra fallas de energías y otras interrupciones contra fallas de servicios?			
¿Los equipos o software cuentan con algún formato vigente donde se autorice su remoción del lugar?			
¿Se aplican medidas de seguridad para todos aquellos activos fuera de la dependencia de sistemas?			
¿Se verifican todos los elementos de quipos que contengan medios de almacenamiento para asegurar cualquier software licenciado instalado en ellos no haya sido retirado?			
Se cuenta con políticas de seguridad para el escritorio limpio, para los papeles y medios de almacenamiento removibles			

Los usuarios se aseguran de que se establezcan protección para los equipos desatendidos?			
total			

Anexo O. Cuestionario Adquisición, desarrollo y mantenimiento de Sistemas

Cuestionario de Adquisición, desarrollo y mantenimiento de Sistemas				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad de la información	Fecha		

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos Generales				
fecha			Proceso auditado	Seguridad de la información Procesos de desarrollo soporte
Día	Mes	año		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se cuenta con la especificación de requisitos para nuevos sistemas de información?			
¿Existen medidas de seguridad para proteger de actividades fraudulentas en los servicios de las aplicaciones para redes públicas?			
¿Existen medidas de protección en cuanto a transacciones de los servicios de aplicaciones?			
¿Cuentan con procedimientos de control de cambios para los sistemas?			
¿Existen revisiones técnicas de las aplicaciones?			
Cuentan con restricciones en los cambios que se realicen en los paquetes de software?			
total			

Anexo P. DOMINIOS DE LA NORMA 27001:2013

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES
POLITICA DE LA SEGURIDAD DE LA INFORMACION	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	Documento de la política de seguridad de la información. Revisión de la política de seguridad de la información.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	gestionar la seguridad de la información dentro de la organización	Compromiso de la dirección con la seguridad de la información. Coordinación de la seguridad de la información. Asignación de responsabilidades para la seguridad de la información. Proceso de autorización para los servicios de procesamiento de información. Acuerdos sobre confidencialidad. Contacto con las autoridades Contacto con grupos de interés especiales Revisión independiente de la seguridad de la información.
	mantener la seguridad de	Identificación de los

	la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas	riesgos relacionados con las partes externas. Consideraciones de la seguridad cuando se trata con los clientes Consideraciones de la seguridad en los acuerdos con terceras partes
GESTION DE ACTIVOS	Lograr y mantener la protección adecuada de los activos organizacionales.	Inventario de activos Propiedad de los activos Uso aceptable de los activos.
	Asegurar que la información recibe el nivel de protección adecuado.	Directrices de clasificación Etiquetado y manejo de información
SEGURIDAD DE LOS RECURSOS HUMANOS	Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.	Roles y responsabilidades Selección Términos y condiciones laborales
	Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que	Responsabilidades de la dirección. Educación, formación y concientización sobre la seguridad de la información. Proceso disciplinario.

	reducir el riesgo de error humano.	
	Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.	Responsabilidades en la terminación. Devolución de activos Retiro de los derechos de acceso
SEGURIDAD FISICA Y DEL ENTORNO	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.	Perímetro de seguridad física Controles de acceso físico Seguridad de oficinas recintos e instalaciones Protección a contra amenazas ambientales. Trabajo en áreas seguras Áreas de carga, despacho y acceso público.
	Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.	Ubicación y protección de los equipos. Servicios de suministro Seguridad del cableado. Mantenimiento de los equipos Seguridad de los equipos fuera de las instalaciones. Seguridad en la reutilización o eliminación de los equipos. Retiro de activos
GESTION DE COMUNICACIÓN Y OPERACIONES	Asegurar la operación correcta y segura de los servicios de procesamiento de información.	Documentación de los procedimientos de operación. Gestión del cambio Distribución de funciones Separación de las instalaciones de desarrollo, ensayo y operación
	Implementar y mantener	Prestación del servicio.

	un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.	Monitoreo y revisión de los servicios por terceras partes. Gestión de los cambios en los servicios por terceras partes.
	minimizar el riesgo de fallas de los sistemas	Gestión de la capacidad Aceptación del sistema
	proteger la integridad del software y de la información	Controles contra códigos maliciosos. Controles contra códigos móviles.
	mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información	Respaldo de la información
	Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.	Controles de las redes Seguridad de los servicios de la red.
	evitar la divulgación , modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.	Gestión de los medios removibles. Eliminación de los medios. Procedimientos para el manejo de la información. Seguridad de la documentación del sistema.
	mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa	Políticas y procedimientos para el intercambio de información Acuerdos para el intercambio Medios físicos en tránsito.

		Mensajería electrónica. Sistemas de información del negocio.
	Garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.	Comercio electrónico Transacciones en línea. Información disponible al público.
	Detectar actividades de procesamiento de la información no autorizadas.	Registros de auditorias Monitoreo del uso del sistema Protección de la información del registro Registros del administrador y del operador Registro de fallas Sincronización de relojes.
CONTROL DE ACCESO	Controlar el acceso a la información.	Política de control de acceso
	Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.	Registro de usuarios Gestión de privilegios Gestión de contraseñas para usuarios Revisión de los derechos de acceso de los usuarios.
	Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.	Uso de contraseñas Equipo de usuario desatendido Política de escritorio despejado y de pantalla despejada.
	Evitar el acceso no autorizado a servicios en red.	Política de uso de los servicios de red Autenticación de usuarios para conexiones externas Identificación de los equipos en las redes Protección de los puertos de configuración y diagnóstico remoto Separación en las redes

		Control de conexión a las redes. Control de enrutamiento en la red.
	Evitar el acceso no autorizado a los sistemas operativos.	Procedimientos de ingreso seguros. Identificación y autenticación de usuarios. Sistema de gestión de contraseñas. Uso de las utilidades del sistema. Tiempo de inactividad de la sesión. Limitación del tiempo de conexión.
	Evitar el acceso no autorizado a la información contenida en los sistemas de información	Restricción de acceso a la información. Aislamiento de sistemas sensibles.
	Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.	Computación y comunicaciones móviles. Trabajo remoto
ADQUISICION,DESARROLLO Y MANTENIMIENTOS DE SISTEMAS DE INFORMACION	garantizar que la seguridad es parte integral de los sistemas de información	Análisis y especificación de los requisitos de seguridad
	evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.	Validación de los datos de entrada. Control de procesamiento interno. Integridad del mensaje. Validación de los datos de salida.
	Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.	Política sobre el uso de controles criptográficos. Gestión de llaves.

	Garantizar la seguridad de los archivos del sistema.	Control del software operativo. Protección de los datos de prueba del sistema. Control de acceso al código fuente de los programas
	Mantener la seguridad del software y de la información del sistema de aplicaciones	Procedimientos de control de cambios. Revisión técnica de las aplicaciones después de los cambios en el sistema operativo. Restricciones en los cambios a los paquetes de software. Fuga de información Desarrollo de software contratado externamente
	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas	Control de vulnerabilidades técnicas
GESTION DE INCIDENTES DE SEGUIRDAD DE LA INFORMACION	Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	Reporte sobre los eventos de seguridad de la información. Reporte sobre las debilidades de la seguridad
	Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.	Responsabilidades y procedimientos Aprendizaje debido a los incidentes de seguridad de la información. Recolección de evidencia
GESTION DE LA CONTINUIDAD DEL NEGOCIO	Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

	críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.	continuidad del negocio y evaluación de riesgos Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información. Estructura para la planificación de la continuidad del negocio. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
CUMPLIMIENTO	Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.	Identificación de la legislación aplicable. Derechos de propiedad intelectual (DPI). Protección de los registros de la organización. Protección de los datos y privacidad de la información personal. Prevención del uso inadecuado de los servicios de procesamiento de información. Reglamentación de los controles criptográficos
	Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.	Cumplimiento con las políticas y normas de seguridad. Verificación del cumplimiento técnico.
	Maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.	Controles de auditoría de los sistemas de información. Protección de las herramientas de auditoría de los sistemas de información.

Anexo Q. Cuestionarios Escaneados

Cuestionario Politicas de Seguridad de la Informacion				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Políticas de seguridad	Fecha Junio	02	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Medidas, controles, procedimientos, normas y estándares de seguridad Contraseñas Autorización del personal
Día	Mes	año		
02	06	15		
Auditor o auditores			Leidy Contreras.	

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
1. ¿Existen medidas, controles, procedimiento o estándares de seguridad?	X		
2. ¿existe un documento donde se encuentre especificado las funciones y obligaciones del personal?	X		
3. ¿Existen procedimientos de realización de copias de seguridad y de la recuperación de datos?	X		
4. ¿Existe un periodo máximo de utilización de las contraseñas?	X		
5. ¿Existe una relación de usuarios autorizados para acceder a los sistemas e incluye los accesos permitidos a los cuales debes acceder?	X		
6. ¿Existen procedimientos de asignación o distribución de contraseñas?	X		
7. ¿El sistema de autenticación de usuario guarda las contraseñas con encriptación?		X	
8. ¿Existe un documento de seguridad donde las personas guardan su contraseña?		X	
9. ¿El sistema de Información esta habilitado para todas las cuentas de usuario en un periodo máximo de vigencia para la contraseña?		X	
10. ¿existen medidas de seguridad en cuanto a la mensajería electrónica?	X		

11. ¿Existe documento de confidencialidad y divulgación?			
12. ¿Existen tratamientos de seguridad de acuerdo con los proveedores?		X	
total			

Cuestionario de control de base de datos				
AUDITOR LKY2	Auditoria de seguridad de la Información	Proceso: Norma ISO 27001:2013		
	Bases de Datos	Fecha Junio	02	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad de la Información Bases de Datos Seguridad de la Información
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?	X		
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?	X		
¿Son gestionados los perfiles de estos usuarios por el administrador?	X		
¿Son gestionados los accesos a las instancias de la Base de Datos?	X		
¿Las instancias que contienen el repositorio, tienen acceso restringido?	X		
¿Se renuevan las claves de los usuarios de la Base de Datos?		X	
¿Posee la base de datos un diseño físico y lógico?	X		
¿Posee el diccionario de datos un diseño físico y lógico?		X	
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?		X	
¿Las copias de seguridad se efectúan diariamente?	X		
¿Las copias de seguridad son encriptadas. ?		X	
¿Se ha probado restaurar alguna vez una copia de seguridad, para	X		

probar que las mismas se encuentren bien hechas?			
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?		X	
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	X		
¿Cuando se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	X		
¿Es eliminada la cuenta del usuario en dicho procedimiento?		X	
¿Hay algún procedimiento para dar de baja a un usuario?		X	
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		
TOTAL			

Cuestionario de Redes y Comunicaciones				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Redes y Comunicaciones	Fecha Junio	02	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Evaluación Infraestructura de redes de comunicación Instalación y diseño de redes
Día	Mes	año		
02	06	15.		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se gestiona la infraestructura de la red inalámbrica en base a los recursos de radiofrecuencia de los clientes?		X	
¿Los enlaces de la red se testean frecuentemente?	X		
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?	X		
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	X		
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	X		
¿Las direcciones IP de los equipos de cómputo son implementadas de forma fija?	X		
¿Cuentan con conmutadores en red, para la expansión de redes locales?		X	
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?		X	

¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	X		
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?	X		
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?	X		
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y Encontrar posibles fallas?		X	
¿Cuentan con administración interna de la red es decir, ¿cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?	X		
¿Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?	X		
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?	X		
¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?	X		
¿Existen grupos de servicios de información, usuarios y sistemas de información que se separen por redes?		X	

Cuestionario de Seguridad física y del Entorno				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Física y del Entorno	Fecha		
		Junio	02	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad física
Día	Mes	año		
02	06	15.		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se tienen lugares de acceso restringido?		X	
¿Poseen mecanismos de seguridad para el acceso a estos lugares?		X	
¿Tiene medidas implementadas ante la falla del sistema de seguridad?	X		
¿Se actualizan las claves o credenciales de acceso frecuentemente?	X		
¿Se tiene un registro de las personas que ingresan a las instalaciones?		X	
TOTAL			

Cuestionario de Seguridad de Equipos				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Equipos	Fecha Junio	02	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	equipos
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Los equipos están ubicados y protegidos para reducir las amenazas y peligros del entorno?	X		
¿Los equipos cuentan con protección contra fallas de energías y otras interrupciones contra fallas de servicios?	X		
¿Los equipos o software cuentan con algún formato vigente donde se autorice su remoción del lugar?		X	
¿Se aplican medidas de seguridad para todos aquellos activos fuera de la dependencia de sistemas?		X	
¿Se verifican todos los elementos de quipos que contengan medios de almacenamiento para asegurar cualquier software licenciado instalado en ellos no haya sido retirado?	X		
¿Se cuenta con políticas de seguridad para el escritorio limpio, para los papeles y medios de almacenamiento removibles?	X		
¿Se aseguran que los usuarios establezcan protección para los equipos desatendidos?	X		
total			

Cuestionario de Adquisición, desarrollo y mantenimiento de Sistemas				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad de la información	Fecha Junio	02	2015.

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos Generales				
fecha			Proceso auditado	Seguridad de la información Procesos de desarrollo soporte
Día	Mes	año		
02	06	15.		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se cuenta con la especificación de requisitos para nuevos sistemas de información?		X	
¿Existen medidas de seguridad para proteger de actividades fraudulentas en los servicios de las aplicaciones para redes públicas?	X		
¿Existen medidas de protección en cuanto a transacciones de los servicios de aplicaciones?	X		
¿Cuentan con procedimientos de control de cambios para los sistemas?	X		
¿Existen revisiones técnicas de las aplicaciones?	X		
¿Cuentan con restricciones en los cambios que se realicen en los paquetes de software?	X		
total			

Cuestionario Politicas de Seguridad de la Informacion				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Políticas de seguridad	Fecha 02	06	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Medidas, controles, procedimientos, normas y estándares de seguridad Contraseñas Autorización del personal
Día	Mes	año		
02	06	2015		
Auditor o auditores			leidy Contreras.	

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
1. ¿Existen medidas, controles, procedimiento o estándares de seguridad?	X		
2. ¿existe un documento donde se encuentre especificado las funciones y obligaciones del personal?	X		
3. ¿Existen procedimientos de realización de copias de seguridad y de la recuperación de datos?	X		
4. ¿Existe un periodo máximo de utilización de las contraseñas?	X		
5. ¿Existe una relación de usuarios autorizados para acceder a los sistemas e incluye los accesos permitidos a los cuales debes acceder?	X		
6. ¿Existen procedimientos de asignación o distribución de contraseñas?	X		
7. ¿El sistema de autenticación de usuario guarda las contraseñas con encriptación?		X	
8. ¿Existe un documento de seguridad donde las personas guardan su contraseña?		X	
9. ¿El sistema de Información esta habilitado para todas las cuentas de usuario en un periodo máximo de vigencia para la contraseña?		X	
10. ¿existen medidas de seguridad en cuanto a la mensajería electrónica?		X	

11. ¿Existe documento de confidencialidad y divulgación?		X	
12. ¿Existen tratamientos de seguridad de acuerdo con los proveedores?		X	
total			

Cuestionario de control de base de datos				
AUDITOR LKY2	Auditoria de seguridad de la Información	Proceso: Norma ISO 27001:2013		
	Bases de Datos	Fecha 02	06	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad de la Información Bases de Datos Seguridad de la Información
Día	Mes	año		
02	06	2015		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?	X		
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?	X		
¿Son gestionados los perfiles de estos usuarios por el administrador?	X		
¿Son gestionados los accesos a las instancias de la Base de Datos?	X		
¿Las instancias que contienen el repositorio, tienen acceso restringido?		X	
¿Se renuevan las claves de los usuarios de la Base de Datos?		X	
¿Posee la base de datos un diseño físico y lógico?	X		
¿Posee el diccionario de datos un diseño físico y lógico?		X	
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?		X	
¿Las copias de seguridad se efectúan diariamente?		X	
¿Las copias de seguridad son encriptadas. ?		X	
¿Se ha probado restaurar alguna vez una copia de seguridad, para	X		

probar que las mismas se encuentren bien hechas?			
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?		X	
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	X		
¿Cuando se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	X		
¿Es eliminada la cuenta del usuario en dicho procedimiento?		X	
¿Hay algún procedimiento para dar de baja a un usuario?		X	
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		
TOTAL			

Cuestionario de Redes y Comunicaciones				
AUDITOR LKV2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Redes y Comunicaciones	Fecha 02	Junio	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Evaluación Infraestructura de redes de comunicación Instalación y diseño de redes
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se gestiona la infraestructura de la red inalámbrica en base a los recursos de radiofrecuencia de los clientes?	X		
¿Los enlaces de la red se testean frecuentemente?	X		
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?			X
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	X		
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	X		
¿Las direcciones IP de los equipos de cómputo son implementadas de forma fija?	X		
¿Cuentan con conmutadores en red, para la expansión de redes locales?		X	
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?		X	

¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	X		
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?	X		
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?	X		
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y Encontrar posibles fallas?		X	
¿Cuentan con administración interna de la red es decir, ¿cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?	X		
¿Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?	X		
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?	X		
¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?	X		
¿Existen grupos de servicios de información, usuarios y sistemas de información que se separen por redes?		X	

Cuestionario de Seguridad física y del Entorno				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Física y del Entorno	Fecha 02	Junio	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad física
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se tienen lugares de acceso restringido?		X	
¿Poseen mecanismos de seguridad para el acceso a estos lugares?		X	
¿Tiene medidas implementadas ante la falla del sistema de seguridad?	X		
¿Se actualizan las claves o credenciales de acceso frecuentemente?	X		
¿Se tiene un registro de las personas que ingresan a las instalaciones?		X	
TOTAL			

Cuestionario de Seguridad de Equipos				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Equipos	Fecha 02	Junio	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	equipos
Día 02	Mes 06	año 15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Los equipos están ubicados y protegidos para reducir las amenazas y peligros del entorno?	X		
¿Los equipos cuentan con protección contra fallas de energías y otras interrupciones contra fallas de servicios?	X		
¿Los equipos o software cuentan con algún formato vigente donde se autorice su remoción del lugar?		X	
¿Se aplican medidas de seguridad para todos aquellos activos fuera de la dependencia de sistemas?		X	
¿Se verifican todos los elementos de quipos que contengan medios de almacenamiento para asegurar cualquier software licenciado instalado en ellos no haya sido retirado?	X		
¿Se cuenta con políticas de seguridad para el escritorio limpio, para los papeles y medios de almacenamiento removibles?	X		
¿Se aseguran que los usuarios establezcan protección para los equipos desatendidos?	X		
total			

Cuestionario de Adquisición, desarrollo y mantenimiento de Sistemas				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad de la información	Fecha 02	Junio	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos Generales				
fecha			Proceso auditado	Seguridad de la información Procesos de desarrollo soporte
Día	Mes	año		
02	06	2015		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se cuenta con la especificación de requisitos para nuevos sistemas de información?		X	
¿Existen medidas de seguridad para proteger de actividades fraudulentas en los servicios de las aplicaciones para redes públicas?	X		
¿Existen medidas de protección en cuanto a transacciones de los servicios de aplicaciones?		X	
¿Cuentan con procedimientos de control de cambios para los sistemas?	X		
¿Existen revisiones técnicas de las aplicaciones?	X		
¿Cuentan con restricciones en los cambios que se realicen en los paquetes de software?	X		
total			

Cuestionario Politicas de Seguridad de la Informacion				
AUDITOR LKV	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Políticas de seguridad	Fecha 02	06	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Medidas, controles, procedimientos, normas y estándares de seguridad Contraseñas Autorización del personal
Día 02	Mes 06	año 15		
Auditor o auditores			Leidy Cortes S.	

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
1. ¿Existen medidas, controles, procedimiento o estándares de seguridad?	X		
2. ¿existe un documento donde se encuentre especificado las funciones y obligaciones del personal?	X		
3. ¿Existen procedimientos de realización de copias de seguridad y de la recuperación de datos?	X		
4. ¿Existe un periodo máximo de utilización de las contraseñas?	X		
5. ¿Existe una relación de usuarios autorizados para acceder a los sistemas e incluye los accesos permitidos a los cuales debes acceder?	X		
6. ¿Existen procedimientos de asignación o distribución de contraseñas?	X		
7. ¿El sistema de autenticación de usuario guarda las contraseñas con encriptación?	X		
8. ¿Existe un documento de seguridad donde las personas guardan su contraseña?		X	
9. ¿El sistema de Información esta habilitado para todas las cuentas de usuario en un periodo máximo de vigencia para la contraseña?		X	
10. ¿existen medidas de seguridad en cuanto a la mensajería electrónica?	X		

11. ¿Existe documento de confidencialidad y divulgación?		X	
12. ¿Existen tratamientos de seguridad de acuerdo con los proveedores?	X		
total			

Cuestionario de control de base de datos				
AUDITOR LKY2	Auditoria de seguridad de la Información	Proceso: Norma ISO 27001:2013		
	Bases de Datos	Fecha 02	06	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad de la Información Bases de Datos Seguridad de la Información
Día	Mes	año		
02	06	15		
Auditor o auditores			Leidy Contreras	

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?		X	
¿Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuarios?	X		
¿Son gestionados los perfiles de estos usuarios por el administrador?	X		
¿Son gestionados los accesos a las instancias de la Base de Datos?	X		
¿Las instancias que contienen el repositorio, tienen acceso restringido?	X		
¿Se renuevan las claves de los usuarios de la Base de Datos?		X	
¿Posee la base de datos un diseño físico y lógico?	X		
¿Posee el diccionario de datos un diseño físico y lógico?		X	
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?		X	
¿Las copias de seguridad se efectúan diariamente?	X		
¿Las copias de seguridad son encriptadas. ?	X		
¿Se ha probado restaurar alguna vez una copia de seguridad, para	X		

probar que las mismas se encuentren bien hechas?			
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	X		
¿Cuando se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?		X	
¿Es eliminada la cuenta del usuario en dicho procedimiento?	X		
¿Hay algún procedimiento para dar de baja a un usuario?		X	
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		
TOTAL			

probar que las mismas se encuentren bien hechas?		X	
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	X		
¿Cuando se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?		X	
¿Es eliminada la cuenta del usuario en dicho procedimiento?	X		
¿Hay algún procedimiento para dar de baja a un usuario?		X	
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		
TOTAL			

Cuestionario de Redes y Comunicaciones				
	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Redes y Comunicaciones	Fecha 02	06	2015

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Evaluación Infraestructura de redes de comunicación Instalación y diseño de redes
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se gestiona la infraestructura de la red inalámbrica en base a los recursos de radiofrecuencia de los clientes?	X		
¿Los enlaces de la red se testean frecuentemente?	X		
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?			X
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	X		
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	X		
¿Las direcciones IP de los equipos de cómputo son implementadas de forma fija?	X		
¿Cuentan con conmutadores en red, para la expansión de redes locales?		X	
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?	X		

¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	X		
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?	X		
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?	X		
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿En cuanto a las pruebas del cableado, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y Encontrar posibles fallas?		X	
¿Cuentan con administración interna de la red es decir, ¿cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?	X		
¿Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?	X		
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?	X		
¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?	X		
¿Existen grupos de servicios de información, usuarios y sistemas de información que se separen por redes?		X	

Cuestionario de Seguridad física y del Entorno				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Física y del Entorno	Fecha 02	06	15

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	Seguridad física
Día	Mes	año		
02	06	2015		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se tienen lugares de acceso restringido?	X		
¿Poseen mecanismos de seguridad para el acceso a estos lugares?	X		
¿Tiene medidas implementadas ante la falla del sistema de seguridad?	X		
¿Se actualizan las claves o credenciales de acceso frecuentemente?	X		
¿Se tiene un registro de las personas que ingresan a las instalaciones?		X	
TOTAL			

Cuestionario de Seguridad de Equipos				
AUDITOR LKV2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad Equipos	Fecha 02	06	2015.

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos				
fecha			Proceso auditado	equipos
Día	Mes	año		
02	06	15		
Auditor o auditores				

A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Los equipos están ubicados y protegidos para reducir las amenazas y peligros del entorno?	X		
¿Los equipos cuentan con protección contra fallas de energías y otras interrupciones contra fallas de servicios?	X		
¿Los equipos o software cuentan con algún formato vigente donde se autorice su remoción del lugar?		X	
¿Se aplican medidas de seguridad para todos aquellos activos fuera de la dependencia de sistemas?		X	
¿Se verifican todos los elementos de quipos que contengan medios de almacenamiento para asegurar cualquier software licenciado instalado en ellos no haya sido retirado?		X	
¿Se cuenta con políticas de seguridad para el escritorio limpio, para los papeles y medios de almacenamiento removibles?	X		
¿Se aseguran que los usuarios establezcan protección para los equipos desatendidos?	X		
total			

Cuestionario de Adquisición, desarrollo y mantenimiento de Sistemas				
AUDITOR LKY2	Auditoria de seguridad Informática	Proceso: Norma ISO 27001:2013		
	Seguridad de la información	Fecha 02	06	15

Con el objetivo de evaluar las políticas de seguridad y tener una mejor percepción del funcionamiento de la dependencia de sistemas de Comfaoriente EPS-S se desea conocer sus respectivas opiniones:

Datos Generales				
fecha			Proceso auditado	Seguridad de la información Procesos de desarrollo soporte
Día	Mes	año		
02	06	15		
Auditor o auditores				

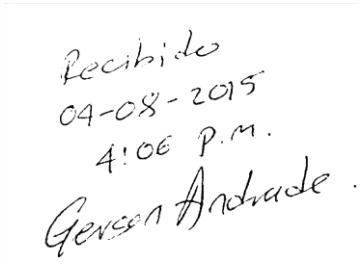
A continuación encontrara una serie de preguntas cuya respuesta se debe señalar con una (X):

Preguntas	SI	NO	N/A
¿Se cuenta con la especificación de requisitos para nuevos sistemas de información?		X	
¿Existen medidas de seguridad para proteger de actividades fraudulentas en los servicios de las aplicaciones para redes públicas?		X	
¿Existen medidas de protección en cuanto a transacciones de los servicios de aplicaciones?		X	
¿Cuentan con procedimientos de control de cambios para los sistemas?	X		
¿Existen revisiones técnicas de las aplicaciones?	X		
¿Cuentan con restricciones en los cambios que se realicen en los paquetes de software?	X		
total			

Anexo R. Informe de Auditoria

San José de Cúcuta 03 de Agosto del 2015

Ingeniero
GERSON ALEXANDER ANDRADE
Jefe Del grupo de sistemas
Comfaoriente EPS-S



Cordial Saludo,

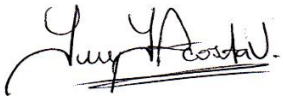
Una vez realizada la auditoria pasiva, con base en el estudio de negocio y la aplicación de cuestionarios a tres funcionarios de la dependencia de sistemas de Comfaoriente Eps-s evaluando algunos dominios de la norma 27001:2013 tales como: Políticas de Seguridad de la información, Organización de la seguridad de la Información, Seguridad de las Comunicaciones, Seguridad física y del Entorno, Seguridad de Equipos, adquisición, desarrollo y mantenimiento de Equipos, se informan las siguientes observaciones o recomendaciones:

Del análisis del negocio que se hizo previamente se observó que la dependencia de sistemas de Comfaoriente Eps-s no cuenta con un organigrama por tanto se recomienda diseñarlo y documentarlo.

De mismo modo se sugiere la adquisición de un nuevo antivirus para los equipos de la dependencia, así como del escaneo programado; la documentación de los inventarios de hardware y de software, La actualización de los controles de cambios del sistema de Información, diseño del proceso de segmentación de la red incluyendo cambios que se puedan presentar en la topología; actualización del plan de contingencia para evitar futuros inconvenientes en caso de presentarse alguna emergencia y puedan ocasionar problemas legales y por último se recomienda implementar un sistema para el registro de las personas que ingresan a la dependencia.

Estas consideraciones están destinadas para ser utilizadas según se estime conveniente.

Atentamente,



VIANNY KARINA BUITRAGO YEINNY YOHANA ACOSTA

YORMAN JOSÉ MÁRQUEZ FUENTES **LEIDY LISBETH CONTRERAS**